Privacy Commissioner

ANNUAL REPORT 1999-2000

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 2000
Cat. No. IP 30-1/2000
ISBN 0-662-64957-5

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at http://www.privcom.gc.ca

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

May 2000

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1999 to March 31, 2000.

Yours sincerely,

Bruce Phillips

Bruce Phillips
Privacy Commissioner

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

May 2000

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1999 to March 31, 2000.

Yours sincerely,

Bruce Phillips

Bruce Phillips
Privacy Commissioner

Acknowledgements

Our thanks to the cartoonists who have enlivened this year's annual report—John Grimes, Cathy Guisewite, and Chris Slane—Peter Lefebvre of CURSOR communications who prepared this year's cover, and Guylaine Duval of Canada Communication Group who supervised the printing of the report.

Pausing to reflect—and soldiering on

Advocating and defending privacy is, most of the time, a labour of love, but it does help sometimes—particularly in the face of adversity—to reflect on exactly what it is that we are trying to do. While all of us have our thoughts on what privacy is and what it means, the following help us to remember why it is important.

Privacy

…the right to be let alone — the most comprehensive of rights, and the right most valued by civilised men.

— U.S. Supreme Court Associate Justice Louis Brandeis, 1928

Conceal your life

— attributed to Neocles, father of Epicure, 3rd century BC

This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain as he sees fit.

— Privacy and Computers, 1972

Knowing what to conceal is knowledge for a king.

— Cardinal Richelieu, statesman, 1640

Civilization is the progress of a society toward privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from man.

— Ayn Rand, author, 1943

My soul has its secrets, my life its mysteries.

— Félix Arvers, poet, 1833

A man has a right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written for the benefit of others, or his eccentricities commented upon, whether in handbills, circulars, catalogues, newspapers or periodicals.

— New York State Court of Appeals Chief Justice Alton B. Parker, 1901

One's true worth is measured by the ability to do alone what one could do in public.

— François de La Rochefoucauld, moralist, 1654

If a society without social justice is not a good society, then a society without privacy is a society without social justice. We must operate in the knowledge that the sanctity of the individual is what we must preserve as if your lives depended upon it — because they do.

—Unknown

It has long been recognized that this freedom not to be compelled to share our confidence with others is the very hallmark of a free society.

— Supreme Court Justice Gerard La Forest, R. v. Duarte, 1990

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

—Professor Alan Westin, 1967

Privacy is related entirely to the degree to which we respect each other as unique individuals, each with our own sets of values which we are entitled to make known or not as we see fit. To truly respect your neighbour, you must grant that person a private life. Respecting one another's privacy means the difference between a life of liberty, autonomy and dignity, and a hollow and intimidating existence under a cloud of constant oppressive surveillance.

— Bruce Phillips, Privacy Commissioner of Canada, 1999

Table of Contents

A Commissioner's Reflections **1**
The Past Ten Years **3**
Bill C-6—Private Sector Data Protection, at Last **23**
Trust and Control: Canadians' Attitudes Towards Privacy **29**
Personal Health Information: Too Many Demands, Too Little Privacy **32**
Progress on the Canada Health Infoway, but what about protection for patients? 36
What's in a name? The Alberta Health Information Act 39
A lifetime medical identification number for physicians 41
Privacy Act Reform **43**
Counting Canadians—Keeping Promises, Building Trust **49**
2001 Census—enhancing transparency in the census collection process 49
Historical census records 52
SIN, Again **57**
A Citizen Profile in all but Name—HRDC's Longitudinal Labour Force File **64**
On the Hill **71**
Cleaning up money laundering: Update on the Proceeds of Crime Act 76
Clearing customs: Flying the unfriendly skies 79
Providing taxpayer/business information to provincial statistical agencies 80
Filling the gaps: A charter of privacy rights 83
Issues Management and Assessment Branch **85**
Assessing Privacy Impacts 85
Data sharing at the Canada Customs and Revenue Agency 87
Conducting client survey research 88
Review of Firearms Registry/Canadian Firearms Centre 91
Data matching proposals—births and deaths with Canada Child Tax Benefit database 92
Incident investigation—loss of laptop in Halifax —Correctional Service Canada 93
Public interest disclosure—medical information about a deceased member of the Canadian Armed Forces 95
Reporting on the administration of the Privacy Act—minimal compliance is not enough 95

Table of Contents (Continued)

Complaints **98**
Definitions of Complaint Findings and Dispositions 101
Advice for all interviewers: Never assume the person sitting across from you can't read upside-down 103
A well-founded complaint about a serious matter—disclosure of personal income tax information 106
"Smith" the good citizen or "Smythe" the criminal? It's all the same to some computer databases 108
Appeal board witness grilled—about irrelevant private matters 110
RCMP officer vs. seatbelt violators: Next, he was going to tell their mothers on them 112
The mystery of the missing missive: Canada Post finds after agreeing to seek 114
Young Offenders Act: Not all matters of privacy are matters for the federal Privacy Commissioner 116
Personal information gets trashed–or so Elections Canada hopes .. 117
Lax information technology procedures in prison cause a dangerous breach of privacy 120
A case about a case, not properly secured 122
Improper destruction of records: A reprehensible act 123
Information access: A matter of give and take 125
The SINs of our fathers: At least some of them will not be visited upon us 127
Partial remission of SIN: a fair compromise, albeit another dubious pun 128
Inquiries 130
In the Courts **138**
Ten years of significant court decisions 138
Ongoing cases 140
Complementing C-6: Private Sector Initiatives **143**
Reclaiming your internet privacy: technology to the rescue! 143
Marketing to children: The Canadian Marketing Association's guidelines 145
Privacy Update **147**
The provinces and territories 147
Privacy around the world 150
Stories we read in the news **154**
Corporate Management **159**
A Tip of the Hat **162**

A Commissioner's Reflections

It is almost ten years since this commissioner took office. This annual report, therefore, is something of a retrospective, summing up some of the major issues and developments of the period.

The report records many improvements, large and small, which have resulted from the efforts of this office. It also shows how far we have yet to go in the ongoing battle to protect the right to a life free of surveillance and intrusion.

Doubtless the recent passage of legislation extending privacy law into the Canadian commercial sector is the most important development of this last decade. It covers a major part of the information world. But it is by no means the whole answer. Still missing is an adequate legal regime covering such things as video surveillance, physical privacy, biomedical privacy, drug and DNA testing, to mention a few.

Also necessary is a revision of the privacy law which governs the information holdings of the Government of Canada. This law, now approaching two decades in age, in some important ways imposes less rigorous standards on government than the new private sector bill does on Canadian business. It should be the other way around. This issue needs to be addressed, urgently.

It's now a cliché that the last ten years have brought forth an information management revolution, thanks to ever more mind-boggling advances in computer and communications technology. It's even more true that the law still lags far behind in its duty to ensure this technology is harnessed to the cause of human liberation and not to its subjugation.

On a personal note, let me say these ten years have given me the greatest privilege and honor I have ever known, namely the chance to go to bat for my fellow Canadians. This office of Parliament, as Teddy Roosevelt would say, is a bully pulpit. Used without fear or favour, dedicated solely to the advancement of human freedom, it can be a powerful voice.

One rueful observation: in ten years, I have yet to meet one person, in public or private life, who has not professed great belief in the right to privacy. But I have witnessed some of those same persons engaged in activities utterly destructive of that right. Talking the talk is no substitute for walking the walk. This job demands a skeptic, albeit an optimist as well.

Finally, it must be said that whatever good we've achieved here in the last decade could not have been done without a truly magnificent staff, as committed and competent a group as I have ever encountered. Their names, past and present, are recorded elsewhere in this report. I am in their debt.

Bruce Phillips
Privacy Commissioner of Canada

The Past Ten Years

Government Rationalization and Privatization
The past decade has seen all levels of government subjected to unrelenting pressures to eliminate waste and manage and deliver public goods and services more efficiently. Governments have responded by contracting out functions once performed by government employees, transferring government operations to the private sector, centralizing and consolidating operations, and striking partnership agreements with other levels of government to deliver services.

Contracting around privacy obligations
These trends, which arguably contribute to more efficient public administration, have also undermined and circumvented the law protecting Canadians' informational privacy rights. Government "contracting out" was the first of these trends, one that prompted us to try to stem the tide of personal information being leaked to the private sector without adequate privacy protection.

We have always argued that once government hires private contractors, they become "agents" for the Crown and thus covered by the *Privacy Act*. However, many contractors neither recognized nor respected this principle, treating the information they gathered or produced as their own. In an effort to stop this end run around the act, we began working with Supply and Services Canada, as it was then called, and Treasury Board to develop model service contracts with clauses specifically designed to bind the contractor to the act. However, years after devising the model contract, our audits continue to reveal contracts without any privacy provisions.

Privatization
Contracting out presented a challenge that was manageable; privatization of significant government holdings was a challenge of another magnitude. The threat to privacy was brought into dramatic relief in 1995 with privatization of Canada's air traffic control system. The creation of NAV CAN saw the transfer of some 6000 federal government employees and the personal files of many more thousands of users of the system out from under the protection of the *Privacy Act*. Their rights to access and control their personal information were gone. Government ignored our repeated recommendations to bind the new entity to the *Privacy Act*, a move we observed "constituted nothing less than a privacy disaster." A lesson may have been learned; the government's transfer of the St. Lawrence Seaway Authority was scrupulously done.

When the federal government was not offloading significant assets, it was merging, centralizing and consolidating government operations under new or reconfigured government departments. A remarkable example of this trend was the 1994 amalgamation of various components of the departments of Employment and Immigration, Health and Welfare, Labour, Multiculturalism and Citizenship, and the Secretary of State under the newly constituted Human Resource Development Canada (HRDC). This new "super department" presides over such vast areas as unemployment insurance, pensions, occupational health and safety, child and family support benefits, disability benefits, education, occupational training, and job creation. This amalgamation brought under one department's control personal information of a nature and on a scale unprecedented in Canadian history. HRDC reaches into virtually every Canadian's life.

Information Management Technology

The explosion in information technology in the 1990s gave the government a new tool in its drive to reduce costs and increase administrative efficiency. In its 1994 *Blueprint for Renewing Government Services Using Information Technology*, the government outlined its plan to use advanced computer technology to "streamline," "re-engineer" and "modernize" the federal public service. The report advocated an integrated electronic web linking all branches of government, based on a standardized and interoperable communications system that would allow federal and provincial governments, as well as private companies delivering government services, to share information.

Anticipating the impact of this technology on citizens' privacy, we developed a "Privacy Check List". The checklist was published in the 1992-93 annual report in an effort to alert senior government officials to the privacy impact of new information management systems, and to guide departments on building privacy into the design and application of these new systems. Although the Blueprint acknowledged the need to ensure the "security, integrity and privacy" of information, in many respects the report's recommendations were a frontal assault on the privacy principles. How, for example, can sharing information across multiple levels of government and the private sector be reconciled with the fundamental privacy tenet that government should only use or disclose personal information for the purpose for which it was collected? We warned that elements of the Blueprint "could

dismantle the protective walls around personal data" erected by the federal *Privacy Act.*

Another advanced data processing technology loomed in the 1990s, the "data warehouse". HRDC was one of the first federal government departments to recognize its potential as an information management tool and to install such a system. A data warehouse integrates data from a variety of different sources and places it in a central electronic repository where the information is standardized and made available for use and manipulation by a number of different users. For managers, the potential is exciting. For privacy, however, the data warehouse rings alarms. Personal information collected for one purpose could become available for different and unrelated purposes. Warehousing data also permits the creation of client profiles—or more insidious—"client intimacy" systems drawn from historical transaction and relationships previously unknown.

Personal Identifiers

The Blueprint's vision of a "horizontally-integrated" public service, and initiatives such as data warehousing, require a unique identifier to link information to the individual. With so many partners in the system, each wants to be sure that they are collecting information about—and delivering services to—the proper person. No surprise then that the whole process of "re-engineering" government would demand a national common client identifier. And no surprise that government would focus on the Social Insurance Number (SIN), already a de facto national identifier through a lack of legislative controls.

In the mid-1990s a group of information technology managers from the income security departments of the federal, provincial and territorial governments began studying the feasibility of a national common client identifier. The group's 1996 report, *Enhancing Service Delivery Through a Common Client Identifier: Options and Opportunities*, concluded that using a common client identifier (and its supporting database) could yield governments significant gains. These gains included properly identifying legitimate claimants before benefits were paid, eliminating duplicated costs from issuing multiple identifiers, and facilitating accurate data matching to detect fraud. Although the group considered several options, it concluded that a "modernized" SIN was the best option. It recommended equipping the SIN card with enhanced security features—including a possible biometric feature to prevent forgery and to accurately link the card to the individual. We could agree with one aspect of the report, its conclusion that privacy was the single greatest barrier to developing a common client identifier.

The Auditor General's 1998 report, *Management of the Social Insurance Number*, confirmed long held suspicions that the existing legislative and administrative framework governing SINs served neither the interests of government nor the privacy rights of the public. Not only did the Auditor General recommend improvements to government management of SINs, he called for Parliament to review the broader policy issues associated with the number, particularly its possible role as a national common client identifier. Parliament responded by directing the Standing Committee on Human Resources Development and the Status of Persons with Disabilities to study both the administration and policy regime governing the SIN. The Standing Committee tabled its report, entitled *Beyond the Numbers: The Future of the Social Insurance Number System in Canada* in the spring of 1999. The committee directed HRDC to prepare a report by year's end that would settle the future role of SIN as national personal identifier.

Privacy concerns have figured prominently in the debate about SIN since its inception. Public resistance to SIN becoming a universal identifier, fortified by the Parliamentary review committee's recommendations in *Open and Shut*, prompted the 1989 Treasury Board directive limiting federal government uses of SIN. Successive Privacy Commissioners have warned of the dangers of establishing any system of universal identification, be it a modified SIN or some other number. We have repeated these warnings but perhaps never more forcefully than in the late 1990s when Canadians faced the real prospect of their government adopting a universal system of client identification.

At the heart of our apprehension is our loss of control: control over what information others have about us, control over how they use that information, control over our ability to influence events and decisions that affect our lives, and ultimately control over our ability to make choices based on our own rational self interest. A universal system of identification threatens to undermine our control by allowing organizations to use the identifier to obtain information about us without our knowledge or consent. It greatly increases governments' ability to gather information from various sources and assemble profiles, as well as to monitor and track an individual's behaviour. When the identifier is compulsory—almost unavoidable when it is widely used and required by all government departments and agencies—the identifier effectively becomes an "internal passport" without which we are nobody. In the "horizontally-integrated" public infrastructure envisioned in the federal government's Blueprint, a universal common client identifier threatens our personal autonomy by exposing our lives to continual scrutiny.

In December 1999, HRDC tabled its position paper on the SIN, entitled *A Commitment to Improvement: The Government of Canada's Social Insurance Number Policy*. To our relief, the paper rejected transforming the SIN into a national personal identifier. HRDC cited two reasons: such a system would be hugely expensive with little evidence of payback; and establishing a comprehensive national system of identification would carry with it "severe privacy concerns". However, the position paper, to be discussed later in this report, did not endorse the Standing Committee's (and our) recommendation to legislate restrictions on SIN, nor did it reject using the number as a common government client identifier. The jury is still out.

Electronic Networks and the Internet

Government's gradual replacement of paper-based records management and communications with electronic systems has led to growing concern over data integrity and security. Unlike conventional mail, information transmitted electronically offers no sealed envelopes to protect confidentiality, and no trusted system to ensure safe delivery. Neither the sender nor the recipient can control (or know) who reads their e-mail while in transit. The privacy implications are obvious for individuals whose personal information is transmitted over open systems. A message sent in the open allows anyone with access to the system to read, record, monitor, tamper with or even destroy the message en route. For employees, it means the threat of supervision through constant electronic surveillance.

To its credit, the Treasury Board Secretariat recognized the implications for employees and developed its *Policy on the Use of Electronic Networks*, published in 1998. The policy clarifies both employers' and employees' expectations and rights when using electronic networks in the workplace. The policy endorses the principle that employees have a reasonable expectation of privacy in their workplace, even if using government equipment. The policy also defines and limits the circumstances in which senior management can legitimately monitor or intercept communications on the government network. Those circumstances include when there are reasonable grounds to suspect an employee of misusing the network, or when monitoring is part of routine network maintenance. Although the policy recognizes employees' right to reasonable privacy in the workplace, it also suggests that an employer could diminish that reasonable expectation simply by notifying employees that monitoring will occur.

Of course, electronic networks threaten the public's privacy when dealing with government through such a system. The federal government commissioned surveys in the mid-1990s to assess the public's comfort level with new interactive technology, and their willingness to use it to deal with

government. The surveys consistently revealed high public anxiety about the security of electronic transactions as well as the systems' ability to protect personal privacy. These findings led the National Advisory Council on the Information Highway, which was developing the federal government's strategy for Canada's information highway, to an inescapable conclusion: assuring the public that electronic transactions are secure from unauthorized access, monitoring, modification and misuse would be critical to government success in modernizing the public service, and preparing the Canadian economy for the information age.

By the late 1990s, encryption was seen as a valuable tool for protecting electronic transmissions. Encryption is the science of transforming plain text into cipher text and vice versa, and is supported by a Public Key Infrastructure (PKI). PKI cryptography is based on a two key system: a public key (known to many) to encrypt the data, and a private key (known only to one party) to decrypt the data. While the keys make a matched pair, one cannot derive the private key from knowing the public key. Thus, no one except the person holding the private key could decrypt the message. This system, combined with a system of digital authentication, holds great promise for protecting security and privacy in electronic communications.

The federal government's system, however, requires some trusted authority to generate the keys, certify their validity, and manage their secure distribution. Here lies the Achille's heel of PKI. To make the system operable, some central authority must know everyone's private key, and hence hold the power to decrypt all our communications. Both Canada Post and the Communications Security Establishment have been touted as the trusted authority. Meanwhile, several federal government departments—Health Canada, Human Resources Development Canada, and Public Works and Government Services Canada—are experimenting with PKI technology. The test results will point the way to its more universal application. However, Canada needs a vigorous debate before government hands any agency the keys to unlock our most private communications.

Surveillance, on the Job and off

In 1992, a senior Office of the Privacy Commissioner manager, addressing a group of human resources professionals, set out an argument for respect for privacy in the workplace, as part of an overall ethical approach to labour relations. His focus was on what might be called the "traditional" threats to privacy in the workplace: excessive demands for employees' personal information, misuse of the information, denial or limitation of access to it, and careless disclosure of it outside the employer's organization. But he also mentioned, in passing, drug testing and genetic testing and a privacy issue

that was just beginning to emerge as a dark side of computerization and electronic information management: electronic surveillance.

Systematic surveillance of workers has a long history, going back at least as far as Frederick Taylor's "scientific management" with its detailed and precise measurements of workers' body movements. The blurring of the line between employers' legitimate interests and employees' private lives also has a long history. Henry Ford, who sent investigators from his "Sociological Department" to workers' homes to report on their moral behaviour, was probably not the first and certainly not the last employer who wanted to look at more than just the result of his employees' work.

Modern times have seen us move beyond searches, background checks, private detectives, medical and psychological testing, and even polygraph testing. The new surveillance includes closed-circuit television systems, keystroke monitoring, computerized surveillance of vehicle use, second-by-second tracking of employee location, and monitoring of telephone, Internet, and e-mail use.

Employers have legitimate reasons, of course, to be concerned about security, trade secrets, reputation, work environment, and possible overloads and crashes of their computer systems. But vigilance should not be confused with hysteria. The surveillance systems they introduce may have consequences far worse than the perceived problem they are set up to address.

Abuse of surveillance systems is an obvious risk. Any system is only as good as the people operating it. Surveillance can creep beyond what is properly the employer's business, to union activities or identification of whistleblowers, for example. Malice can lead to selective building of negative records on particular employees. Sensitive information can end up in the wrong hands, and find its way into blackmail schemes.

But even when surveillance systems are used exactly as intended, they raise troubling questions. Given the length of working days, is it reasonable to put an absolute prohibition on employees communicating privately, without

employer surveillance, with family, friends, and others? Employees who work full-time and live alone may have no choice but to conduct some personal business from the workplace. Moreover, it is inevitable when people work together that they will communicate. Such interaction can make the most boring job bearable—and can be the breeding ground for ideas about how work can be done better. There is also a valid argument that workers need to be able to let out some steam during the daily grind.

In short, we would argue, employees have a legitimate interest in a reasonable quality of work life, and privacy is an essential element of that. This is even more acute with the growth of telework and the fading of the distinction between work and home—and the need to put limits on presumed links between off-duty activities and work performance.

Our complementary roles of monitoring the application of the *Privacy Act* by federal institutions and monitoring developing privacy issues beyond the scope of the act have given us an interesting vantage point. We take some satisfaction in observing that federal institutions have avoided the excesses seen elsewhere.

In the 1992-93 annual report, we reported on the Department of Communications' project to develop a smart card for employees that would be used as a purchase card, allow access to computer files, control high-tech inventory, and replace the employee in/out board. We noted that the most likely government-wide application of a card that could validate identity, employment status, and security clearance would be as a government employee card. The danger would be that such a card could become a tracking device. We observed that the government could devise standards and guidelines that would control its use.

Also in 1992-93, we reported on the Federal Government's Telework project committee, tasked with reporting on a 3-year pilot project allowing employees to work at home and deliver their products to the employer electronically. This was introduced for valid objectives: allowing employees to balance work and home, and reducing energy consumption, pollution, and traffic congestion. But we had concerns about adequate security and privacy safeguards for personal information being worked on in the home and transmitted electronically, and the risk of compromising employees' home lives, by introducing the element of supervision and monitoring into their homes.

In 1994, we reported on the Royal Canadian Mint's monitoring of employee telephone conversations. The Commissioner, although he had reservations,

concluded that the Mint's practice was not in violation of the *Privacy Act*, since the monitoring was for performance evaluation purposes and employees were advised in advance. Nonetheless, the Commissioner reminded the Mint of employees' rights to examine notes made of the monitoring, and recommended that it develop procedures to take account of other privacy concerns, including customers' rights. The Mint took note of his concerns and undertook to address them.

Video surveillance was the subject of a complaint reported in the 1997-1998 annual report. We observed at the time that covert videotaping, as one of the most intrusive tools, demands the most rigorous justification. Concerned about the general privacy issue, the Commissioner wrote to Treasury Board, urging it to develop a government-wide policy on covert surveillance. He recommended that the policy specify, among other things, that surveillance should be based on reasonable suspicion and used only after less intrusive methods had been ruled out, that reasonable expectations of privacy should be respected, and that surveillance should be restricted as much as possible to the person under suspicion, rather than sweeping in employees indiscriminately. These recommendations, while specifically addressing video surveillance, arguably apply to all forms of workplace surveillance.

Some of the Commissioner's concerns about surveillance were addressed by the Treasury Board *Policy on the Use of Electronic Networks*, published in 1998. Although, as noted above, that policy is not without its shortcomings, it did ensure that electronic networks were not the basis of an "electronic sweatshop." And in April, 1999, Treasury Board released a policy on video surveillance, which adopted all the recommendations made by the Commissioner the previous year.

Federal Government workplaces, then, have not become quite the Orwellian world that some had feared. This is due in large part to the long-standing recognition of the principles of fair information practices embodied in the *Privacy Act*, and to the fact that privacy issues are debated and discussed in a legal framework. We might even take some small measure of credit ourselves.

Discussing the surveillance of employees' e-mail and Internet use, a manager was recently quoted as saying, "You live in a democracy; you don't work in one." How absolutely should we accept this? Are we prepared to accept that Canadians, upon entering the workplace, lose all their privacy rights? It is established in Canadian law that certain fundamental human rights are a matter of public policy; they cannot be conjured away by means of an employment contract. Privacy has not yet been recognized in this way by the courts. The Federal Government, to its credit, has listened when we have

made the case, and has recognized that strict legality is one thing, fairness and good management another. With the Office's new responsibilities, we will certainly be looking closely at workplace privacy in the private sector—including not just electronic surveillance, but biomedical issues as well.

Biomedical Technology

Biomedical technology has developed dramatically in the last 10 years, and, as is so often the case with new technology, it is a double-edged sword. We have consistently urged citizens to recognize technology's potential for both good and harm, and to frame decisions about technology around fundamental questions of what kind of society we want.

Genetic mysteries are being solved; the sequencing of the entire human genome is said to be imminent, years ahead of schedule. Yet while this research holds great hope for society's understanding of the genetic components of diseases, it also threatens to engulf us in a wave of information deeply personal, only half-understood, and with the potential for new and invidious forms of discrimination.

The use of DNA analysis for forensic identification, hailed as a breakthrough for both prosecuting criminals and clearing the innocent, also offers the possibility of genetic dossiers on large numbers of citizens.

An upsurge in drug testing—less pronounced in Canada than in the U.S., but significant nonetheless—has given the state and employers unprecedented power to peer into our bodies at random, searching for evidence of socially unacceptable behaviour.

And biometrics—such as digitized fingerprints, retinal scans, and facial recognition technology—press our very bodies into service as personal identifiers, and this intimate, indelible information is then scattered and shared beyond our control.

Genetic testing

Genetic testing and analysis hold great potential for early identification and treatment of those predisposed to particular medical conditions. Genetics may also help employers and employees improve workplace safety and health by screening for genetically linked conditions that could be aggravated by particular environments. Monitoring genetic changes and genetic conditions in the workplace can also help early identification and intervention.

But genetic testing also holds the potential for great harm. Genetic analysis can reveal highly sensitive, intimate information about both the person tested and his or her relatives. Once a person is tested, there is real risk that the results could be used to select and promote genetically "fit" employees and reject the "unfit" and to determine who is eligible for benefits and insurance.

In 1992, we released our *Genetic Testing and Privacy* report, a comprehensive look at the privacy implications of the new technology. The first of our 22 recommendations urged the government to study the extent to which public and private sector employers were conducting genetic tests, and the uses they were making of the information. We also recommended the government adopt legislation to ensure that genetic material was collected within a legal framework, that no one was forced to give up genetic material, that genetic testing would not be a condition of employment, and that no one would suffer discrimination for refusing to be tested. We also proposed amending the definition of personal information in the *Privacy Act* to ensure that it included both genetic samples and the information derived from their analysis.

Virtually all the recommendations have fallen on deaf ears. With the costs for genetic tests falling, a lengthening list of conditions that tests can identify, and pressure building to develop comprehensive linked health information banks on Canadians, we still have no legal framework for this intrusive technology. We do not even know how and how much employers are using genetic testing.

"SIGN HERE, BREATHE HERE, THUMBPRINT HERE, LOCK OF HAIR HERE, SALIVA HERE, SPECIMEN HERE, SAY CHEESE!"

Genetic testing was one of the privacy issues examined by the House Standing Committee on Human Rights and the Status of Persons with Disabilities. In its April 1997 report, the Committee urged the government to take immediate action to deal with privacy violations and discrimination flowing from genetic testing. The Committee envisaged a review of genetic testing policies and practices in the employment, health, insurance, and criminal justice sectors. In addition, the Committee recommended reviewing existing legal instruments, holding public consultations, and developing legislation to specifically address privacy and discrimination issues.

Parliament was dissolved shortly after the Committee delivered its report; thus the government did not respond to the recommendations at that time. The recommendations were later adopted by the Standing Committee on Human Resources Development and the Status of Persons with Disabilities as part of its examination of the administration of the Social Insurance Number. However, the government did not address the issue of genetic testing in responding to this committee's report.

Protection of genetic privacy has received considerably more attention in the United States. A significant number of states have passed laws banning genetic discrimination in employment, insurance, or both. Dissatisfied with patchwork protection, some U.S. legislators are sponsoring Congressional bills with similar provisions to apply to private sector employment and insurance. This February, U.S. President Clinton signed an executive order prohibiting the federal government from conducting mandatory genetic testing of its workforce and discriminating based on genetic information.

Forensic DNA analysis

Forensic DNA testing, one of the most rapidly developing and perhaps best-known areas of biomedical technologies has profound privacy implications. Forensic DNA testing takes bodily substances from suspects or volunteers, analyzes the samples and compares them to biological evidence—skin, hair, blood, or semen found in connection with a crime. Analysis of a suspect's DNA is then compared with DNA found at a crime scene. The results can either eliminate the suspect or establish with a high degree of certainty (although that point is not without its critics) that the two samples match.

DNA matching has been widely applauded as the most important development in criminal identification since fingerprinting. A relatively new and uncertain technique at the beginning of the 1990s, it has recently become high profile, particularly when it produces dramatic proof of innocence and a wrongful conviction as in the David Milgaard and Guy Paul Morin cases. Not so high profile, however, has been the subtle trend towards capturing and retaining DNA information about an increasingly large segment of the population.

We can support using DNA evidence, but reject a forensic investigation tool evolving into a national file of biological identifiers. Of particular concern is banking not just results, but also the samples themselves. Maintaining a bank of samples from a segment of the population virtually begs using the genetic material for research and other unrelated purposes. Reports from the U.S. indicate that pressure is building to retest samples so that "markers"— race, gender, physical characteristics, potential psychiatric disorders—can be

added to the identification data to which DNA data banks are presently limited.

Forensic DNA evidence was first used in Canada in 1988, but there was no legislation to authorize law enforcement officers taking DNA samples from suspects until 1995, when Parliament amended the *Criminal Code* to permit obtaining samples under warrant. Soon after, the Solicitor General began consultations on creating a national DNA data bank to facilitate criminal investigations. The data bank would hold samples and analyses from crime scenes and from those convicted of a range of offences. The Solicitor General's discussion papers noted many of the privacy implications pointed out in *Genetic Testing and Privacy*.

We urged that the data bank be limited to results of analysis and not include biological samples. We also asked that the range of offences be limited to violent offences for which future DNA evidence would likely be available. However, several groups and politicians pressed to expand collection to include taking DNA samples automatically when the person is charged with an indictable offence, just as fingerprints are now. This would have led to collecting DNA for offences as minor—and as unlikely to yield any DNA evidence—as swearing a false affidavit.

When the *DNA Identification Act* finally passed in December 1998, it included some, though not all, of our recommendations. The forensic DNA data bank will include both the analyses and the samples themselves, and the range of offences is broader than we think necessary. Nonetheless, many of our recommendations prompted privacy protections in the legislation, not least of which was a prohibition (clarified in later amendments) against using genetic material for anything other than forensic identification purposes. This should reduce the risk of "function creep." Amendments introduced late in 1999, but not yet passed, would require the RCMP Commissioner to report to the Solicitor General every year on the operation of the DNA data bank; the Solicitor General will then table the report in Parliament. An advisory committee, of which the Privacy Commissioner is a member, will oversee the bank's operations.

We commend the government's cautious approach in the face of heavy pressure to expand forensic DNA sampling and analysis. Late in 1999, the International Association of Police Chiefs, which represents police agencies in 112 countries, urged legislatures to pass laws requiring DNA samples from anyone arrested on any charge, whether the charge was murder, impaired driving, or shoplifting. In Britain, the Lothian and Borders Police instituted a

program of genetic sampling of people charged with any offence, including routine traffic violations.

The greatest danger of a forensic DNA data bank is its potential to engulf a significant part of the population and become a genetic population register. Recovering abducted children, assisting adults with amnesia, providing security for Alzheimer's patients: all could be offered as justification for extending genetic sampling—and would blur the line between forensic and non-forensic uses.

More than ten years ago, Gary T. Marx, a U.S. academic with a special interest in privacy and surveillance, looked at then-recent but burgeoning forensic DNA testing. He highlighted the danger of what he called "surveillance creep"; what was once a serious intrusion comes to be accepted as business as usual. New uses are found for surveillance systems until the new technology has put us into the twilight zone so aptly described by U.S. Justice William O. Douglas: "As night-fall does not come at once, neither does oppression....It is in such twilight that we all must be most aware of change in the air—however slight—lest we become unwitting victims of the darkness."

Drug testing

Twelve years after we first rang the alarm against drug tests creeping over the border and into Canadian workplaces, we have not changed our minds. Drug testing is a serious privacy intrusion that is justified neither by the problem it purports to address nor by any evidence of its effectiveness. A positive drug test result does not reveal past or present impairment or a risk of impairment. It does not show how much the person took or when. In fact, it does not even confirm that the person took the drug. What it does show is that, at some point, the person came into contact with the drug. And a *negative* drug test does not establish that a person has *not* taken a drug because drug metabolites take several hours to appear in urine. Education, support, and treatment are the most effective approaches to drug abuse. Sometimes improving working conditions can help employees' problems; far better to help employees recognize risks and seek help than to treat them all as suspects.

Drug testing was already an important privacy issue at the beginning of the 1990s. U.S. President Reagan's 1986 order for mandatory random drug testing of federal government employees started U.S. citizens down the road to widespread testing. Canada has not followed the lead of the U.S., but there were calls for drug testing from various quarters within both government and the private sector. The Office of the Privacy Commissioner responded to

these calls with a vigorous defence of privacy in the report, *Drug Testing and Privacy*.

At the time that report was written, Transport Canada had proposed mandatory random drug testing for workers in surface, air, and marine transportation, the Minister of National Defence had announced mandatory random tests for Canadian Forces members, and Correctional Services Canada was testing prisoners in federal penitentiaries. The report looked at those programs, at drug testing and its rationale, at the *Privacy Act*, and at the broader privacy implications.

We concluded that the justifications offered for drug testing generally, and mandatory random testing particularly, did not withstand close scrutiny. The lack of evidence of a serious drug problem, and existing evidence that testing was ineffective in enhancing workplace safety, did not justify its extreme intrusiveness.

Whether the report had influence or not, Transport Canada abandoned its plan to test transportation workers, and the government has not introduced anything similar since, much less tried to extend drug testing as has the U.S. government. The Canadian Forces abandoned its random testing program in 1995.

They may all have saved themselves some trouble. Drug testing suffered two significant legal setbacks in the 1990s. In 1996, Imperial Oil's drug and alcohol policy was found by an Ontario Human Rights Board of Inquiry to contravene the *Ontario Human Rights Code*. The decision was upheld by the Ontario Court General Division in February 1998; Imperial Oil's appeal to the next level is still pending. The Imperial Oil decision was particularly significant because it concerned work in the highly dangerous environment of an oil refinery. The courts found nonetheless that the company could deal with the safety risks without resorting to random drug testing. In July 1998, the Federal Court of Appeal ruled that the Toronto Dominion Bank's policy of testing new and returning employees contravened the *Canadian Human Rights Act*. TD has abandoned the policy.

Pressures for drug testing have not disappeared, due in part to the increasing integration of the Canadian and U.S. economies. Perhaps the most significant example came in 1996 with the application of U.S. regulations requiring drug testing of all truck drivers, regardless of nationality, who operate vehicles on U.S. highways. Any Canadian trucking company that uses U.S. roads at any point must now conduct mandatory random drug testing. In 1998, apparently inspired by U.S. law, a Senate special committee examining

transportation safety and security recommended random drug and alcohol testing in Canada. (The Committee dissolved without issuing a final report, so it is unknown how the Government would have responded.)

Measures to improve public safety are welcomed. Were the proponents of drug testing able to demonstrate that these programs actually reveal impairment as breath-alcohol testing does, or that there is a significant drug problem in the transportation workforce, or that drug testing significantly reduces risk, our conclusions might be different. But that is not what we see. Without a demonstrable positive effect on public safety, all we are left with is a humiliating intrusion into workers' private lives.

Canada has not followed the trend in the U.S. where in 1996, according to an American Management Association study, 81 per cent of major firms tested their employees for drugs. However, we have seen some parroting of American rhetoric, and its translation into action; Ontario tests social assistance recipients for drugs and imposes mandatory treatment on those who test positive. This mirrors similar American programs, where the war on drugs and the demonization of social assistance recipients have become potent tools for demagogues. So far, no one has challenged the tests before the Ontario courts, but it seems likely that someone will. Ontario law considers drug dependence a disability, and refusing services such as social assistance benefits on the basis of a disability is prohibited

A satirical article in a 1998 *Privacy Journal* proposed guidelines for parents on drug testing their children. One of the difficulties, the author suggested, was that children might turn the tables and test their parents. His solution? Parents should be sure to lecture children about the importance of communication and trust in the family. The point, while ironic, should be kept in mind by those concerned about substance abuse in schools, workplaces, and society generally.

Biometrics

While it is early to say that we have seen a revolution, we have witnessed a trend in the way we verify and authenticate people's identity: from something you *have*, such as a card, through something you *know*, such as password or PIN, to something you *are*: biometrics.

Using technology that scans and measures physical or behavioural characteristics such as fingerprints, facial features, or voice, iris, or retinal patterns to authenticate identity, was first introduced in the 1970s. However, in most people's experience biometrics was virtually science fiction at the

beginning of the 1990s. A series of performance failures in the 1980s sent industry in other directions—to keypads, access cards, and PINs.

But interest resumed early in the 1990s. Sales of biometric devices, excluding those for law-enforcement use, more than doubled in 1991. The increase may have reflected price decreases; in 1995, according to an industry report, the "average price per access point protected" dropped under $2,000 from more than $6,000 five years earlier. The report predicted that "$500 and under devices may help make biometrics a more common sight in daily life." By 1998, a U.S. company was selling fingerprint scanners for $99.

As the cost of the technology drops, what once was an idle wish becomes a pressing need; what used to be a fantasy becomes a reality. We hear almost daily of some new use for biometric technologies—in automated banking, policing, computer security, administering social benefits, and preventing school truancy.

In the early 1990s, the U.S. Immigration and Naturalization Service introduced a new travel document to speed passengers pre-clearing customs at Pearson International Airport in Toronto. The card was imbedded with the pattern of the bearer's hand; electronic readers in the airport could authenticate the identity of a traveller by matching the image on the card with the traveller. This use of biometrics appeared to be designed with some privacy considerations since the biometric image is stored in the card, not in a government record.

Later in the decade, a more problematic application surfaced: Metro Toronto's decision to require social assistance recipients to carry a smart card containing their digitized fingerprints. The cards would be credited with social assistance payments, and then could be used as debit cards for direct payment in stores. As we noted in an earlier report, the problem with this system lies largely in its potential to provide a database for unrelated uses—for example, for social science research into social assistance recipients' spending habits. The system eventually approved for all municipalities uses biometrics for identification only, not for debit cards, and includes a number of important privacy protections. But the problem remains, fingerprinting is associated with criminality. And once again, social assistance recipients are singled out for treatment that no other citizens suffer—and arguably, that no other citizens *would* suffer.

By the end of the 1990s, news about biometrics was everywhere. In December 1998, the *Globe and Mail* reported that a Toronto fitness club controlled members' admissions by scanning handprints, and Disney World used fingerprint scanners to identify annual pass holders. The *Globe* cited a U.S. estimate of $500 million spent worldwide on biometric devices in the previous year, with one-third of the sales to the private sector. The *Globe* predicted that sales of fingerprint devices alone would rise to $1 billion in 2001, from $145 million in 1997. Early this year, the *Financial Post* reported that an Australian technology and investment company was preparing to launch a voice-recognition feature for its on-line trading business. It also reported that an iris-recognition system would soon control employee access at a U.S. airport, and a Canadian bank is beginning to use fingerprint readers for a similar purpose. Another Canadian company plans to develop a computer mouse that will identify users' fingerprints for on-line banking. Chicago's O'Hare International Airport uses fingerprint biometrics to control access in its baggage handling areas. And the *Post* also reported that an American hospital had installed a finger-recognition system that helps speed up registration of patients, prevents fraudulent insurance claims, and gives hospital staff immediate access to patients' medical records. The same company makes a system that controls access to computers by verifying fingerprints.

Privacy advocates have frequently called attention to the privacy implications of biometrics—both collecting, using, and storing this intimate personal information, and the potential it offers for matching different activities and transactions through a single identifier. But the public has yet to be engaged in a serious debate.

Biometric technology offers unquestionable advantages. Authenticating identity, regardless of how it is done, is often critical, particularly as more businesses move more operations onto the Internet. Unlike passwords, a biometric identifier cannot be given away, lost, or forgotten. If technology can ensure that limited funds for social benefits and assistance are available only to those who are genuinely entitled, surely this helps, rather than hurts, social assistance recipients. With sensitive issues such as health information—and for that matter, receiving social assistance—a biometric identifier can provide highly secure storage. And who can argue with controlling employee access, especially in safety-critical operations like airports?

But the accuracy of biometrics combined with their falling cost can be seductive, leading people to seek and eventually require proof of identity where none is really needed. Many activities can be done anonymously, just

as most cash transactions are now; there is no need to identify the parties. As with identity cards—as with all systems of identification—we need to be careful about letting occasional necessity lead to casual optional use, which in turn prompts suspicion and eventually exclusion of those who refuse to identify themselves when it is unnecessary.

A further problem with biometrics is its integration into the authentication system required for electronic commerce, and particularly a public key infrastructure. The system would store biometric features with a "trusted third party", which would issue digital identity-verification certificates. Who will be the third party we are supposed to trust? When we exchange security for privacy—for example, giving up our name, address, social insurance number, and other personal information in exchange for a digital certificate—we cannot retrieve the privacy we have surrendered. But when we entrust indelible, unchangeable, and highly personal individual markers drawn from our physical selves to another, the risk to us and the burden on the recipient are far greater.

Biometrics is intimately tied, not just to proving identity but also to surveillance. It may be as simple as using fingerprint-controlled access to computers to verify that employees are checking in when they say. Or it could be much more: facial recognition technology, a biometric application touted as useful for controlling access, is also the basis of video surveillance systems that can pick individual faces out of crowds. In fact, video surveillance is making facial recognition one of the fastest growing markets in biometrics. According to the *Globe and Mail*, a recently developed system enables driver's licence bureaus to match a face with a record in a database of 1.5 million images. And *The 1997 Advanced Card and Identification Technology Sourcebook* noted, apparently with approval and no intended irony, that the same facial recognition technology that would permit screening social assistance databases for duplicates and airport lounges for terrorists would also likely enable your multimedia PC to recognize you for teleconferencing on the electronic superhighway.

Privacy Act Reform

Government restructuring and the development of advanced information, surveillance and biomedical technologies are all sorely testing the efficacy of the *Privacy Act;* a law written in the information technology dark ages of the early 1980s. Although the act has proven to be fairly adaptable, it is fast becoming creaky. We have tried to keep our fingers on its pulse and report regularly on developing aches and pains but it is clear that what the act needs is not some nips and tucks but major surgery.

The entire scope of the legislation needs changing to make it live up to its name. In 1998, we began a comprehensive in-house review of the legislation. That review, discussed later in this report, was completed late in 1999 and contains more than 100 recommendations designed to prepare the act for the staggering challenges ahead. With its work on Bill C-6 largely over, Parliament now needs to return to where it all began—protecting Canadians' privacy against a well meaning, some would say zealous, state.

Bill C-6

It seems fitting to conclude this ten-year review by commenting on the *Personal Information Protection and Electronic Documents Act*, the highlight of this Commissioner's term. (The act is discussed in more detail in the section that follows.) For several years, this Office has been urging the federal government to pass legislation to protect Canadians' privacy rights in the private sector. With the legislation a reality, we are now looking forward to the challenge of fulfilling the Privacy Commissioner's mandate as established by the act.

We have stated many times that, of all the clauses in the act, none is more important than the one that requires the Privacy Commissioner to promote understanding and knowledge about privacy. One of our goals will be to inform Canadians about their rights, and about threats to their privacy, including the personal and social consequences of privacy intrusions. We want to do more than inform and educate; we intend to make the Office of the Privacy Commissioner a place where Canadians can turn for assistance when they feel deprived of a privacy right.

We also stand ready to help the business community. We recognize that businesses will need time to learn how to work with this legislation just as we will need time to learn how business works. Businesses are understandably concerned about how the act will affect their companies and how the Privacy Commissioner will exercise the Office's authority. While we will do everything we can to avoid impeding business, we do not want to convey the impression that nothing will change. Many businesses, we expect, will have to adjust their personal information practices to meet the obligations set out in the act. More than anything else, what is most needed is a new consciousness on the part of businesses about personal information. This information must be seen not as just another resource—in some cases a company's most important resource—but as an asset over which business can never claim complete ownership. In short, businesses must become trustees.

Bill C-6—Private Sector Data Protection, at Last

Parliament's passage of the *Personal Information Protection and Electronic Documents Act* has taken Canada a major step forward in protecting its citizens' privacy rights. This landmark law puts Canada into the enviable ranks of leading industrialized nations that have recognized the need for privacy regulations in the private sector.

Public interest in privacy protection has grown steadily over the past two decades, prompted by social, economic and technological change. The development of a global economy, proliferating computer networks, exponential growth in Internet transactions, satellite-based telecommunications, and sophisticated surveillance technologies all contributed to a general public uneasiness about eroding personal privacy.

The Canadian government's first response to calls to protect personal information—or data protection, as it is frequently called in Europe—was to include limited privacy protection in Part IV of the 1978 *Canadian Human Rights Act*. But Part IV provided far from comprehensive data protection; it focused on limiting access to records and lacked controls on government collection, use and disclosure of personal information. In 1982, Parliament enacted the *Privacy Act*, which extended privacy protection to most but not all of the federal public sector, as of July 1, 1983.

In 1984, Canada joined 22 other industrialized nations in adhering to the Organization for Economic Cooperation and Development's *Guidelines for the*

Protection of Privacy and Transborder Flows of Personal Data. The OECD guidelines were intended to harmonize data protection laws and practices among member countries by establishing minimum standards for handling personal data in each country. The guidelines were not enforceable, but they were a benchmark and a starting point for creating data protection legislation in a number of countries around the world.

The federal *Privacy Act* and equivalent provincial legislation have largely fulfilled Canada's commitment to establish fair information practices for the handling of personal information in the public sector. However, until the government introduced the *Personal Information Protection and Electronic Documents Act* in 1998, little had been done, except in Quebec, to protect Canadians' privacy rights in the private sector. The *Personal Information Protection and Electronic Documents Act* addresses this deficiency.

So it has taken almost two decades for Canada to extend to the private sector the fair information practices embodied in the OECD guidelines and the *Privacy Act*. Private sector opposition to legislation, a lack of will on the part of the government, the inability to reach a consensus on how best to protect personal information in the private sector, and the changing technological environment are but some of the explanations for the delay.

Prompted in part by the OECD Guidelines, and possibly by the fear of what might follow if they did not act, the private sector took the initiative in the 1980s, introducing privacy codes to address growing public concern about the actual or potential misuse of personal information gathered during commercial transactions. The life insurance industry led the way in 1980 with "Right to Privacy" guidelines; the banks, the direct marketing industry, computer companies, and the telecommunications industry followed. Although welcome, these codes and guidelines did not provide comprehensive privacy protection. In particular, these voluntary codes do not provide for an independent oversight body to monitor their implementation and receive complaints from consumers.

In 1991, a CSA International (formerly the Canadian Standards Association) committee made up of business, consumer, government, and labour representatives began work on a model privacy code for the private sector. Using the OECD Guidelines as a starting point, the committee agreed on a draft model code that was circulated for comment at the end of 1994 and approved by the stakeholders in 1996.

While supporting the CSA process and other voluntary initiatives, the Privacy Commissioner was becoming convinced that goodwill alone was not enough.

In 1992, he lobbied two Senate committees in support of changes to the *Bank Act* that would empower the Governor in Council to regulate the collection, use and disclosure of customer information, and the inclusion of the protection of privacy as a policy objective in the *Telecommunications Act.* Commenting on CSA's draft model code in the 1994-95 annual report, the Privacy Commissioner observed, "The greatest significance of the CSA Code may lie, not in its proposed form as a voluntary code for business, but in its embodiment into national framework legislation—a national standard of privacy against which all sectors can be held accountable."

Several new developments contributed to the Commissioner's belief that comprehensive legislation was needed: growing commercial trade in customer information; evidence that customers' information was being collected, used and disclosed without their knowledge or consent even in industries that had adopted voluntary privacy codes; wide variations in the protection provided by privacy codes in different industries; continuing lack of a truly effective oversight body in any industry using voluntary codes; and, finally, Quebec's passage of privacy protection law for the private sector.

In 1995, the Canadian Direct Marketing Association called on Parliament to use the CSA's model privacy code as the basis for legislation. In his response to the Information Highway Advisory Council's recommendation that private sector privacy protection was needed, Industry Minister John Manley announced that the federal government would introduce such legislation. In 1996, Justice Minister Allan Rock reiterated this pledge before a meeting of the world's privacy commissioners, promising that legislation controlling the federally regulated private sector would be in place by the year 2000.

Meanwhile, the *European Union Data Protection Directive* came into force in October 1998. The Directive established EU data protection standards thus facilitating transfers of personal data among EU member countries. But the EU Directive also imposes an "adequacy" test on non-member countries. EU members may only transfer personal data to other countries such as Canada, if that country ensures an adequate level of protection.

These events culminated in the government tabling Bill C-54, the *Personal Information Protection and Electronic Documents Act*, in the fall of 1998. The introduction of this bill was one of the most significant milestones in the history of privacy protection in this country. The law regulates commercial uses of personal information, requiring business to respect a code of fair information practices. Equally important, it provides an independent oversight of business practice—mandating the Privacy Commissioner to investigate complaints, issue reports and conduct audits. As a last resort, it

provides individuals with recourse to the Federal Court and empowers the Court to award damages.

Finally, it gives the Commissioner a broad mandate to promote the act through public education and research. The Privacy Commissioner's office has struggled over the years to inform Canadians about their privacy rights and developments that strengthen or threaten those rights. Yet there has been no formal authority for the Commissioner to conduct public education. The bill addresses this deficiency, requiring the Commissioner to develop and conduct programs to foster public understanding and recognition of the purposes of the bill.

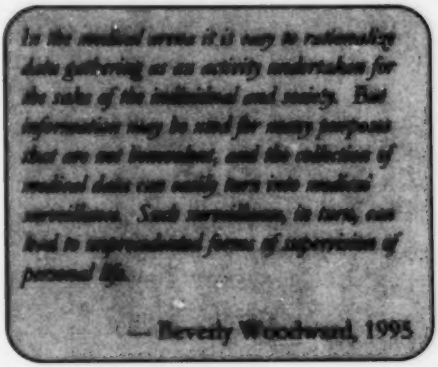
After its introduction in the fall of 1998, the Commons Standing Committee on Industry held extensive hearings on the bill; about 60 witnesses representing business, associations, academics, consumers and the privacy community appeared. Representations fell into two main categories: business, which felt that it was too rigorous; and consumer and civil rights groups who argued it was too gentle. At the end of the hearings, the Committee's report to Parliament made more than 20 recommendations. These ranged from adding a primacy clause and a reasonable person test, defining publicly available information by regulation, adding some circumstances where information might be disclosed without consent, and whistleblower protection. The House accepted all the Committee's recommendations.

Parliament rose for the 1999 summer recess leaving the *Personal Information Protection and Electronic Documents Act* at Report Stage in the House of Commons. With the start of a new session in October, the bill was mentioned in the Throne Speech and re-introduced as Bill C-6, returning to Report Stage.

The parties in the House moved a substantial number of motions. The amendments provided exclusions for the law enforcement community, extended coverage to the non-profit sector on barter and sale of lists and clarified the act's operation in the first three years. The latter amendment added the phrase "discloses the information outside the province **for consideration**" (emphasis added) to clarify the circumstances in which provincially regulated organizations would be subject to the act during the first three years. The House of Commons passed the bill, with these amendments, on October 26, 1999.

The bill then moved to the Senate's Standing Committee on Social Affairs, Science & Technology. The committee heard at length from the healthcare community and concluded that it was the only sector that was not part of the

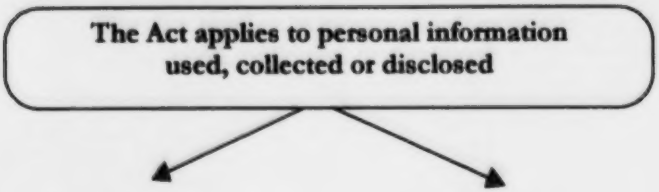
broad consensus supporting the bill. In fact, the healthcare sector itself was divided: one part recommending tougher provisions on patient consent and subsequent uses of personal health information, the other arguing that the bill would constrain operational activities in the healthcare sector. Faced with such divergent views, the Committee recommended delaying application of the law to personal health information for one year after the bill comes into force. This allows the healthcare community and governments approximately two years to determine how to manage personal health information used in commercial activities.



The Senate passed the bill in December with this amendment and a related one defining personal health information. "Personal health information" was defined as information concerning the physical or mental health of an individual, living or dead, and information collected in the course of, or incidental to, providing health services to the individual. The definition also includes information concerning an individual's donation of any body part or bodily substance, as well as information derived from medical tests. These amendments were approved by Parliament on April 4, 2000.

Some businesses have expressed uneasiness about the act and the Privacy Commissioner's role, worrying that compliance will cost them time or money. However, the Commissioner has made a commitment to help business adjust to the new legislation and will take a cautious and even-handed approach to its implementation. Business can ease the transition by handling personal information with care before the law comes into force, and reviewing and revising their information handling to meet the standards set out in the act. Businesses that can demonstrate respect for their customers' privacy will avoid complaints and reap the rewards of greater customer confidence.

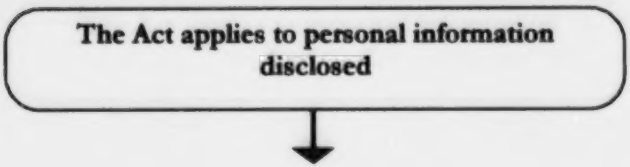
INITIAL APPLICATION OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT



By a federal business in the course of a commercial activity

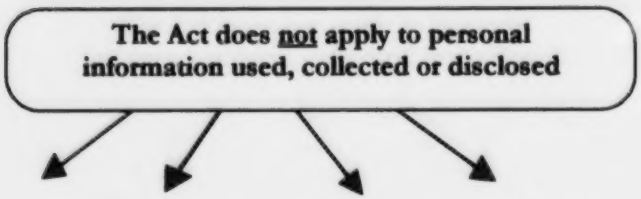
By a federal business about their employees

- One year deferral for personal health information



Outside the province for consideration

- One year deferral for personal health information



By an individual for a personal purpose

By an organization for a journalistic, artistic or literary purpose

By an organization outside the course of commercial activity

Within a province, except for commercial activit of a federal business

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership of other fundraising lists.

Federal business means any organization within the legislative authority of Parliament.

Trust and Control: Canadians' Attitudes Towards Privacy

Surveying people about privacy is a challenge—those most likely to be concerned are least likely to answer the questions, and many consider calls from survey firms to be intrusive. As well, respondents (and most Canadians) may simply not be aware of the steady erosion of their privacy. When businesses and governments use hidden cameras, "cookies," data matching and e-mail monitoring to collect personal information and monitor their employees, customers, or citizens, they seldom issue press releases. To borrow the old saw about obscenity—"I know it when I see it"—people may know a privacy invasion when they see it, but they probably cannot see it.

Nevertheless, surveys are still the most effective way to assess people's views. We have always been keenly interested in Canadians' attitudes towards privacy; we were one of the sponsors of the first comprehensive privacy study, *Privacy Revealed: The Canadian Privacy Survey*, conducted by EKOS Research Associates Inc in 1992.

In 1999, we participated in another EKOS study, *Rethinking the Information Highway: Privacy, Access and the Shifting Marketplace*. The study had a broad scope—attitudes towards privacy were just one of the topics covered. Other topics included access to communication technologies, use of the Internet, and Canadians' willingness to use the Internet to access government services. The study was comprised of two separate surveys: one with a random sample of 5,014 Canadians aged 16 and over in June 1999, and a second follow up survey in late fall 1999 of 1,830 participants from the first survey. The results of the two surveys are considered to be statistically accurate +/- 1.4 percentage points and +/- 2.3 percentage points, 19 times out of 20 respectively.

In general, Canadians appear to be less concerned about privacy than they were in the 1992 study. By 1999, 47 per cent of Canadians agreed with the statement, "I feel that I have less personal privacy in my daily life than I did ten years ago," compared with 60 per cent in 1992. The number of Canadians who agreed with the statement, "There is no real privacy because government can learn anything it wants about you," dropped to 63 per cent from 81 per cent. The number of Canadians who agreed with a similar statement about business dropped to 57 per cent from 71 per cent.

The 1999 study suggests that Canadians are also becoming more sophisticated in their attitudes towards privacy. Fifty per cent said that they

now "feel confident that they have enough information to know how new technology might affect their personal privacy", up from 43 per cent in 1992.

A majority of Canadians (54 per cent) don't mind companies using personal information as long as they know about it and can stop it. Canadians may be willing to provide personal information in certain circumstances, and may even be willing to sacrifice some of their privacy, but they want to know what they are getting in return. One thing they want is control.

Canadians demonstrated a surprising willingness to make privacy tradeoffs in return for tangible benefits. Forty-two per cent of respondents said that they would agree to having their grocery shopping habits monitored, allowing the store to develop a client profile, in return for a 10 per cent discount on their groceries. Slightly more than a third of Internet users (36 per cent) would agree to having their online habits monitored by a reputable company in return for a new computer and free Internet access. Nevertheless, even these very significant benefits were not enough to convince a majority of Canadians to trade away their privacy. The two questions assume that the people involved in such programs would be fully informed of the personal information being collected and how it is being used. In the real world of customer loyalty programs, this is rarely the case.

The survey asked a number of related questions about Canadians' willingness to accept potential privacy intrusions that could further public policy objectives such as helping criminal investigations or reducing abuse of social programs. A bare majority (51 per cent) believes that governments should be able to link databases to ensure that individuals are not cheating on social programs, while 44 per cent oppose such data-matching activities because it would allow governments to monitor individuals. Sixty-one per cent agree that law enforcement officials need to be able to monitor e-mails during criminal investigations. Fifty-five per cent of Canadians agreed with the

concept of creating electronic networks of health records on the assumption that it would improve health care. On the other hand, a majority of Canadians (55 per cent) believe that governments collect more information than they need to provide services.

Canadians appear to be very comfortable providing certain types of information to one organization, but extremely uncomfortable with another. For example, the study found that while only 19 per cent of Canadians were "extremely" concerned about providing personal information to doctors or hospitals, the proportion climbed to 27 per cent for governments, 40 per cent for polling and research companies, 49 per cent for Internet service providers and 62 per cent for telemarketing companies.

Overall, Canadians' willingness to provide personal information depends on several factors; understanding what is being done with the information and why, their trust in the organizations collecting the information, and the resulting benefits.

The survey revealed that Canadians have substantial concerns about the ability of business and governments to protect personal information provided over the Internet. For example, Canadian Internet users were only "somewhat confident" on average that any organization would be able to fully protect personal information submitted online. Likewise, only 12 per cent of Canadians said that they would be willing to give their credit card number over the Internet to make a purchase.

What does all this mean? Clearly, privacy is a very complex issue and many Canadians remain very concerned. There is also a growing emphasis on security issues; Canadians want to make sure that personal information is safe. And they are deeply divided on government initiatives that may trade off privacy protection in favour of improved health care or greater efficiency. More than four out of ten Canadians opposed the storage of health records on a secure electronic network even when the question suggested that it would improve health care. The Office of the Privacy Commissioner believes that the relatively small majority support for these initiatives is a weak justification for ignoring the real concerns, not to mention the privacy rights, of significant numbers of Canadians.

Personal Health Information: Too Many Demands, Too Little Privacy

Patients' privacy is steadily eroding in the name of health research, ready access to personal information and administrative efficiency—and Canadians are the last to know. A recent survey conducted for the Canadian Medical Association (CMA) revealed that three out of four Canadians believe that the information they give their doctor is kept confidential. The reality is far different; the lineup behind our doctors—all claiming to "need to know"—is long and growing.

Personal health information stored in electronic systems is becoming fair game for bureaucrats, researchers, as well as insurance and pharmaceutical companies, among others. Many such organizations are already surreptitiously collecting and using personal health information without even the courtesy of telling us that our lives are being categorized and our records dissected.

And technology offers new ways of amassing health information without our consent. For example, many Net surfers now do background research on medical conditions and treatments for friends and family on the Web. Who would have thought that many health-related web sites, despite promises to protect site visitors' privacy, actually share the information they collect? A recent survey of 21 sites by the California HealthCare Foundation revealed just that.

We should also be sceptical of the protection reputedly offered by so-called "anonymized" health information. American computer scientist Latanya Sweeney demonstrates that simply removing identifying details from patient records will not assure their privacy; the resulting data only appear anonymous. Ms. Sweeney argues that retaining too many patient-specific facts, particularly when they refer to a rare condition or unusual procedure, can identify individuals. The resulting data can also be linked or matched with information from separate sources, like a birth date or postal code, to identify people in an "inferential disclosure".

Researchers and bureaucrats frequently make the appalling argument that

patients would never agree to having their information used in research if they were asked. But current survey data finds the opposite. In fact, the CMA survey revealed that almost eight out of ten Canadians either strongly or somewhat agreed that they would allow their personal health information to be released to governments and researchers, but *only* if their consent were sought. Without consent, 51 per cent of Canadians would *not* agree to release their personal health information even if any identifying information were removed. Governments and researchers take note.

Protecting patients' privacy is critical to the success of electronic health networks; reminding proponents seems a truly endless task. For all the benefits these initiatives promise, they pose other substantial risks including possible inaccuracy. Dr. Denise Nagel, Executive Director of the U.S. National Coalition for Patient Rights observed that

> ...coerced data are not reliable data. Patients who know their health care records will be viewed by legions of strangers and non-strangers will not be truthful. They will have an incentive to omit details or fail to see a doctor at all if they feel a breach of confidentiality will have serious consequences.

Until quite recently, patients were categorically denied access to their own medical records—apparently they could not be trusted with too much information. How offensive that view seems today. Yet the same argument is made; patients are not competent to decide whether to provide their personal health information for research or administrative uses.

Among the vaunted benefits of a health information network are grandiose promises of better health care. Yet advocates offer few specific examples of real benefits (beyond virtually instant delivery of a patient's record to an emergency room). Health information networks might well help Canadians receive better healthcare in the long run. In the short run, the risks to patient confidentiality outweigh the benefits. We can and must eliminate those risks—one of which is that without proper privacy safeguards, the networks could fail from patient distrust.

To gain that trust, health related organizations and government agencies have a lot of questions to answer. For one, they must begin to explain how health information flows from the patient's primary care physician to all the secondary users. Despite repeated requests, no one seems able to chart that flow. It is difficult to have a meaningful discussion about the privacy implications of any proposed health network when all we have are generalities about what happens now.

And we all have to be clear on the definitions of the terms we use. For example, an inability to distinguish privacy from confidentiality, and both from security, is a critical misunderstanding. Ensuring confidentiality and security does not necessarily protect privacy.

Privacy is the right to be let alone, to be free from interference, from surveillance and from intrusions. It is a human right that a former Supreme Court Justice described as "at the heart of liberty in a modern state". Infringements on privacy are infringements on liberty and autonomy. To protect privacy in a health context could mean not collecting information at all.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting it; the relationship is built on an assurance that the information will not be disclosed without the person's permission. Confidentiality assumes information has been provided.

Security is the technology or administrative arrangements organizations use to prevent confidential information from being disclosed. It too assumes there is information to protect.

Being clear on other key definitions is also important. For example, at a May 1999 meeting on the proposed National Health Surveillance System, some participants used the term "data collectors" to mean a provincial government, laboratory or health authority. Others took it to mean the primary care physician. Even the architects of the health networks do not seem to be speaking the same language.

And even if we do manage to speak the same language, we have many issues yet to resolve. For example, of all the arguments challenging the practicality of patient privacy that need rejecting, opposition to consent is one of the most important. As Donald Haines of the American Civil Liberties Union stated in 1996, "Medical information is like the patient's right arm, and abuse of such information would be more deleterious than abuse of the arm. Whatever you wouldn't do to the right arm without patient consent, you

shouldn't do to the medical information about the patient". To be able to trust any health network, we need governments to commit to making patient privacy a priority. For example, last year's annual report recommended spending some Canada Health Infoway funds to determine how the Canadian Medical Association's Health Information Privacy Code could be implemented. The CMA Code (described as a "Hippocratic Oath for the Information Age") is an excellent model for all players to emulate. Unfortunately, few are willing to consider the substantial privacy opportunities the Code offers.

Although certainly not as comprehensive as the CMA Code, a recent private member's bill by MP Greg Thompson sends the right message. His proposed *Patients' Bill of Rights* (Bill C-417) would give patients a right to examine and correct their health records and, better yet, the right to have their health records kept confidential unless they provide written and informed consent. The bill calls for a uniform approach by making federal funding for provincial health care contingent upon protecting and promoting patient rights.

We should also note that the Standing Senate Committee on Social Affairs, Science and Technology is currently examining the state of the health care system in Canada and expects to submit its final report by December 2001. The Committee will study

- The fundamental principles on which the publicly funded health care system is based;
- The historical development of the health care system;
- Publicly funded health care systems in foreign jurisdictions;
- The pressures and constraints on the health care system; and
- The role of the federal government in the health care system.

We look forward to presenting our views to the Committee.

Public policy makers must ensure that future discussions about health information privacy are as open and as broad as possible if they want to move the debate forward. For a successful model they need only consider the democratic process that went into preparing the 1997 report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities entitled *Privacy: Where Do We Draw the Line?* The committee, chaired by the Hon. Sheila Finestone, did not just go through the motions: the process took 10 months and truly advanced knowledge and

understanding about privacy issues in this country. It is now almost five years since that committee began its study. Surely some Health Infoway funds could be used to establish a similar consultation process on health information privacy. Achieving consensus on this issue demands involvement of the public, privacy and patient advocates, health professionals, health-related government agencies, labs, pharmacists, and all the rest. The patients at the heart of this system deserve no less.

Progress on the Canada Health Infoway, but what about protection for patients?

The Advisory Council on Health Infostructure was established in 1997 to provide the Minister of Health with recommendations on the development of a strategy for a national health infostructure. The Council's mandate ended with the release of its Final Report last February. It's fair to say that we were pleased with several of the Council's recommendations. As we reported last year, the Council acknowledged the critical importance of privacy, citing it as one of the four strategic goals to be met when building the networks. The Council also supported specific health privacy legislation and identified the essential components of any such legislation. It also endorsed harmonizing privacy protection across all jurisdictions and specifically cautioned against sinking to the lowest common denominator. We look forward to Health Minister Allan Rock's response to the Council's Final Report.

The Commissioner wrote to the minister and the Advisory Council commenting on the Final Report and the implementation document—the *Health Information Roadmap: Responding to Needs* —that was released shortly after. The minister replied, "Health Canada gives privacy issues serious consideration" and "a Departmental Committee on Privacy of Health Information is being established to ensure that Health Canada adopts a consistent approach to the protection of health information". He also observed, "privacy is one of the forefront issues in our legislative renewal exercise". All this is good news indeed, if only we could be assured that the level of privacy protection would be consistently high.

Despite Minister Rock's assurances, the Canadian Institute for Health Information (CIHI) and Statistics Canada quietly released a troubling new implementation document entitled *Roadmap Initiative...Launching the Process* in January, which it will continue updating on the CIHI web site at http://www.cihi.ca/Roadmap/Launch_process.htm.

CIHI is a federally chartered but independent, not-for-profit organization. It works with Health Canada and Statistics Canada, bringing together programs from the Hospital Medical Records Institute (HMRI), the MIS Group, Health Canada (Health Information Division) and Statistics Canada (Health Statistics Division).

This new Roadmap document envisions CIHI simply monitoring progress in different jurisdictions and revisiting its existing privacy policies and procedures to see if changes are necessary. This hands-off approach seems to conflict directly with the Advisory Council's recommendations on privacy and the Minister of Health's assurances.

The latest version of the Roadmap summarizes proposals for—or expansion of—36 projects. Privacy is further watered down from the version accompanying the Advisory Council's Final Report early last year, where it was virtually absent. For example, the new version's concept of "person oriented information" to track individual encounters with the health system and non-health determinants is more detailed and ambitious. Just what is the difference between "person oriented information" and information that identifies particular individuals? It looks like another distinction without a difference.

The latest Roadmap makes several proposals that raise significant privacy concerns, for example,

- Establishing unique national identifiers for patients, facilities and service providers;
- Introducing national standards for reporting prescription (and the potential for tracking non-prescription) drug use;
- Collecting more detailed information in Vital Statistics registries; and
- Collecting more information through various disease and incident registries.

The Roadmap states that privacy, confidentiality and security issues are going to be dealt with under the Infrastructure component of the "strategic

framework" being used to guide the developments.

It is troubling that Health Infoway projects are proceeding without, at the very least, the protection that the minister's own Advisory Council recommended for Canadians. And, as mentioned earlier, no Health Infoway funds have been provided to assess the impact of implementing the Canadian Medical Association's Health Information Privacy Code. And we await details from the various Health Infoway projects to chart the information exchanges. Until everyone understands what databases officials contemplate linking, no one can assess the privacy risks these linkages pose.

The Advisory Committee on Health Infostructure and the Privacy Working Group17 April 2000

In contrast to the "watch and wait" approach to privacy advocated by CIHI and Statistics Canada in the Roadmap, consultations for some action are underway among the federal, provincial and territorial F/P/T health officials.

The Conference of Deputy Ministers of Health is supported by a new F/P/T Advisory Committee on Health Infostructure. (This F/P/T Advisory "Committee" is distinct from the Advisory "Council", which ceased to exist following the release of its Final Report last February.)

The F/P/T Advisory Committee's mandate is to develop national strategies to enhance the use of communications technologies and information in the health sector. It has four working groups—privacy, surveillance, telehealth, and strategic planning. A fifth group may be formed to examine electronic health records.

Apparently, the privacy working group has been negotiating a "harmonization accord" or "resolution" for the Deputy Ministers of Health. The resolution would have each province and territory identify gaps in its own privacy protection, then take any additional action it considered necessary.

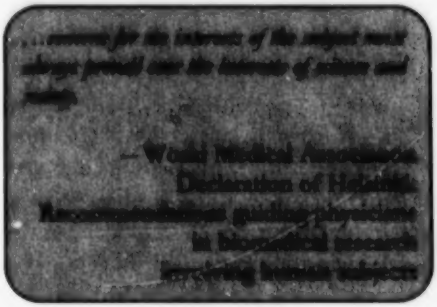
More protection is needed—there is cause for alarm. For example, a government-commissioned KPMG study of British Columbia's Pharmanet (the computer network of residents' prescription drug histories) revealed that too many people have access to this confidential and sensitive data. More recently, the fate of Manitoba's SmartHealth projects, such as building the Health Information Network, have been called into question by allegations of mismanagement. In a climate of such uncertainty, citizens can be forgiven for wondering whether governments are giving top priority to protecting their personal health information.

With these examples in mind, the privacy working group would do well to consult privacy advocates before finalizing this resolution. We await the call.

The National Health Surveillance Network

The health surveillance working group—one of the four working groups mentioned above —reports to the Advisory Committee on Health Infostructure.

At their June meeting in Charlottetown, federal, provincial and territorial Deputy Ministers of Health formally endorsed a proposal to develop a health surveillance network for Canada.



In our comments to Health Canada officials, we objected to many aspects of the proposal, most of which concern tracking people's lifestyles and specifically "family, economic, cultural and social circumstances". Individuals must retain the right to decide whether to participate in such a health surveillance system. Individual choice is an essential component of privacy protection that must be preserved, particularly when the network's objectives include health promotion and well-being, not simply protecting the public against imminent health risks.

Health Canada is developing a web site for the health surveillance network to inform the public about various surveillance projects. Another source of information on the projects is "HealthSurv.news", the Network for Health Surveillance in Canada newsletter at health_surveillance@hc-sc.gc.ca or call 1-888-288-2098.

What's in a name? The Alberta Health Information Act

Alberta's new *Health Information Act* (previously known as Bill 40) received Royal Assent on December 9th. The Act gives individuals a right of access to their personal health information, sets rules for the collection, use

and disclosure of this information and provides for independent review by the Alberta Information and Privacy Commissioner.

While the Alberta law is less comprehensive than provisions in Saskatchewan's *Health Information Protection Act* (passed last year), it requires any "custodian" (i.e., any person or organization that controls health information) wanting to disclose an identifiable individual's diagnostic, treatment and care information by electronic means to first obtain the individual's consent. Given the popularity of electronic patient records and development of Alberta's we//net—a system to integrate provincial health information—we hope that provisions that give patients control over having their information put on a network or transmitted electronically will become more important.

Alberta's Information and Privacy Commissioner Robert Clark has reviewed the legislation and, while he does not oppose it, he has identified several problems. In fact, Mr. Clark observed that "Bill 40 is not a privacy act: it is an information act which provides for disclosure of information under controlled conditions". And there was vocal opposition to this bill by several groups, including the Alberta Medical Association. Among other concerns, the AMA objected that Bill 40

- does not meet the standard in the Canadian Medical Association's Health Information Privacy Code, which the AMA has endorsed;
- fundamentally changes the doctor/patient relationship;
- compromises physicians' ability to safeguard patient records in their offices; and
- redefines patient consent for therapeutic reasons to encompass a broad range of activities not directly related to the medical care of the patient.

The doctors raised important concerns. The act does not require individuals' consent for the collection, use and disclosure of their personal health information in seventeen situations. Examples include avoiding or minimizing an imminent danger to the health or safety of any person and detecting or preventing fraud. The act also does not apply to such private sector organizations as insurance companies, and there is no prohibition or sanction for collecting or using the personal health number for purposes other than health care. As well, the Minister, the Department of Health and Wellness, a Provincial Health Board, a Regional Health Authority, and the Alberta Cancer Board may ask any custodian to provide individually identifying health information. The act then allows these custodians, in turn, to further disclose the information to a number of other custodians.

One of the most troubling aspects of the new Alberta act is that it allows any custodian to develop a family or genetic history for any purpose at all, without asking patients for their consent or even informing them of this practice. The objective appears to be a massive collection and storage of this information until a researcher finds a use for it, with no established limits. This sort of unbridled tracking of personal information is particularly disturbing. What, if any, limits are there to the kind of information that could interest these researchers? Groups of people—entire families and their generations to come—can be stigmatized by health bureaucrats, insurance companies and employers using their personal health information against them.

Perhaps most revealing about the purpose and spirit of the *Alberta Health Information Act* is the removal of the word "protection" from the title (its 1997 title was *Health Information Protection Act*). What's in a name indeed?

A lifetime medical identification number for physicians

Medical students, residents and physicians in Canada will soon have a new unique lifetime identification number. According to the organizations developing the system (the Federation for Medical Licensing Authorities for Canada, the Medical Council of Canada and the Association of Canadian Medical Colleges) the nine-digit identifier will only identify the physician. It will not contain any other coded information such as specialty or licence status. These organizations argue that the identifier is needed because there are problems accurately identifying physicians. The process to assign identification numbers will be in place in several provinces starting in April 2000.

Although we asked the federation to reconsider developing this identifier, favoring other administrative fixes, we commend it for seeking our input in the first place. Asking for the privacy community's views on this type of project demonstrates sensitivity to privacy other organizations would do well to emulate. It remains to be seen how much impact our comments had on the original proposal.

We made several suggestions. For example, past experience has shown that personal information in an accessible form is subject to "function creep". Despite protections built into any system, the mere existence of the number will prompt creative and unrelated uses. Once all medical students and physicians are issued a number, there is a real likelihood of unauthorized access to their personal information using this number as the key. And when

many organizations use any common identifier, the possibility increases that information from disparate sources will be combined into comprehensive profiles. Unique personal identifiers and powerful technologies may appear to solve immediate administrative problems but they pose long-term threats to individuals' privacy, a fundamental value in a democratic society.

Privacy Act Reform

When the federal *Privacy Act* was drafted in 1982, government anticipated the need to review the legislation periodically to ensure it remained relevant and effective. This was the rationale for section 75, which required a Parliamentary review three years after the act came into force, and permanently thereafter. Parliament's comprehensive 1986 review of both the *Privacy Act* and the *Access to Information Act* produced the seminal document *Open and Shut: Enhancing the Right to Know and the Right to Privacy* in 1987. *Open and Shut* made more than 100 recommendations for improving the act, none of which were translated into law. However, several recommendations appeared as policy directives, most notably those on data matching and restricting government uses of the Social Insurance Number.

More than a decade has passed since Parliament turned its mind to the *Privacy Act*—14 years in which the information environment has been literally transformed by the Internet, DNA testing (and other biotechnologies), data warehousing and government downsizing. Some of these challenge the very foundation of the act. We have not been shy to point out where it has proved to be wanting; throughout the 1990s the Privacy Commissioner has recommended numerous changes to the law. These have not been acted upon and the act creaks on.

The weaknesses are all the more striking now that Parliament has passed the *Personal Information Protection and Electronics Documents Act*. This act (which regulates personal information handling in the private sector) contains many features that are superior to the *Privacy Act*, making a comprehensive review of the existing law both urgent and unavoidable.

With this in mind, we began a comprehensive review of the act, aiming to develop a set of concrete recommendations for its modernization and improvement. The review was completed in December 1999 and produced more than 100 recommendations. We highlight the more significant ones here; the complete report will be available by the summer of 2000.

Give the act primacy

Although we argue that the *Privacy Act* is an overarching statute since it defends a fundamental human right, the act is far from clear on the point. The effect is that government institutions may routinely infringe individuals' privacy rights when another law permits. It is one of the ironies of history that when privacy was protected by the *Canadian Human Rights Act*, which is a statute of general applicability, it enjoyed a quasi-constitutional status that it

arguably does not enjoy now. It is time to rectify the wrong and reassert privacy's rightful place among the fundamental values that underpin our free and democratic society. The *Privacy Act* should clearly state its primacy over all laws dealing with the collection, use and disclosure of personal information.

Make it a true "privacy" law

The *Privacy Act* speaks only about privacy of information. But it is increasingly evident that the state infringes on individuals' privacy in ways that do not collect "personal information" as the act defines it. Two examples are real time electronic monitoring of individuals' behaviour, which may not necessarily generate a "record", and collecting biological samples from individuals, which may not yield personal information on its face. Neither practice is regulated under the existing act. These types of privacy infringements should be no less subject to state control than any other form of information collection. We recommend that the *Privacy Act* 's definition of personal information mirror that of the new *Personal Information Protection and Electronics Documents Act* which is not restricted to "recorded" information.

Clarify disclosures about public servants

Federal public servants' privacy rights have long been a matter of contention between privacy advocates and those defending the public's "right to know" how government manages the state's affairs. The *Privacy Act* does not protect information that "relates to the position or functions of" public servants from disclosure. We do not debate the importance of the public's right to obtain information about government operations, including some information about its employees. However, the act could better balance the public's interest in government accountability and its employees' privacy interests by defining more precisely the type of employees' personal information that could be disclosed.

Classify disclosures—with and without notice

The act is inadequate concerning a government institution's duties when it discloses personal information under the lengthy list in section 8(2). Since this section authorizes disclosure without the individual's consent there should be a corresponding duty on the institution to inform the individual about the disclosure. Clearly some disclosures could not be dependent on a duty to inform the individual before disclosure—for example, disclosures to law enforcement bodies for criminal investigations. But the same cannot be said of all the permitted disclosures. What would be the harm in notifying individuals before their information is given to National Archives for historical purposes? Disclosures should be separated into two categories; those in which prior notification is practicable and reasonable, and those that

may be made without the individual's knowledge.

What purpose would prior notification serve if the government can still disclose personal information without our consent? Some argue there is little point knowing if we can do nothing to prevent it. However, prior notification would empower individuals to challenge a disclosure before it is made. In his 1991-92 annual report, the Privacy Commissioner remarked "the *Access to Information Act* provides a mechanism for alerting third parties, such as corporations, whose sensitive commercial information may be shared. Yet, the *Privacy Act* provides no similar rights to individuals whose sensitive personal information may be disclosed. Does not personal information deserve protection from abuse that is at least the equal of that afforded to corporations?" The question still begs an answer.

Government institutions should be prevented from disclosing personal information when notification is required, until the individual has been given a reasonable opportunity to either consent or object (unless failure to disclose immediately would result in some identifiable harm). The institution could disclose the information over the individual's objections, unless s/he asked the court to review the institution's decision. In that case, as in the federal *Access to Information Act*, the government institution would again be barred from acting until the court reviewed the matter.

Have Privacy Commissioner investigate all personal information complaints

Section 19 of the *Access to Information Act* requires government to deny a request for access when the record in question contains "personal information" as defined in the *Privacy Act*. Thus disclosure is only possible if the *Privacy Act* permits. However, the Information Commissioner now investigates complaints that government has denied a third party access because the information is "personal", thus determining whether the *Privacy Act* has been correctly applied. The Privacy Commissioner's role is limited to being notified if there is a public interest in the disclosure, or if the individual complains to the Commissioner about the disclosure. Herein lies the problem; the body whose mandate is to work in favour of making government information accessible, is charged with interpreting the application of the *Privacy Act* whose mandate is protecting personal information from public access.

The recommendation casts no aspersions on the integrity or competence of the Information Commissioner. Nor does it in any way usurp the Court's role as the ultimate arbiters of the law. Nevertheless, whenever government action discloses personal information in response to an access request, the

Privacy Commissioner, not the Information Commissioner, should investigate any complaints involving personal information.

Expand Court review

A long-standing weakness in the existing federal *Privacy Act* is the individual's limited rights of access to the courts. Individuals may seek a Court review only when a government institution denies them access to their own personal information. The remedies are essentially limited to the Court ordering access to personal information if it determines that access has been improperly denied. This is an unacceptable stricture on citizens' privacy rights. The right of access to one's personal information, while important, is but one of the rights that enable individuals to exert some control over government handling of their information. Restrictions on government collection, use and disclosure are equally—arguably more—important principles that underpin all informational privacy law.

The new *Personal Information Protection and Electronics Documents Act* gives individuals a right to ask the courts to review the collection, use and disclosure of their information by organizations covered by the act, their access to personal information held by these organizations, as well as a right to seek compensation for any damages caused by breaches of the law. (See the discussion of Bill C-6 above.) The disparity between this act and the narrow appeal of the *Privacy Act* is clearly untenable; the public would enjoy fewer rights in their dealings with government than they would with the private sector. The *Privacy Act* needs amending to expand the matters the Court may review and the remedies available to complainants.

Incorporate rules for data matching

The *Privacy Act* has no specific rules governing data matching. Although Treasury Board established guidelines on data matching in 1989, these are simply a policy directive and do not have the force of law. The guidelines require the matching department to submit a detailed proposal for the Privacy Commissioner's review. Given the few proposals submitted, we have long suspected that most data matching is not being reported and thus is invisible to both Commissioner and—more important—the public. Were the duty to report set out in law, government institutions might be more forthcoming or face the consequences.

Simple delinquency may be the cause for the sporadic reporting. It is also probable that government officials do not recognize a procedure as a data match, raising questions about the clarity of the policy directive. Technically a data match is any comparison of personal information collected from different sources for different purposes. This would include matches to confirm that information contained in one database corresponds to that of another. It is highly likely that bureaucrats do not recognize this kind of data confirmation as a proper data match. While data matches of this kind ("up-front" matches) might be less privacy intrusive when individuals are notified, they are no less a match and should be reported.

Data matching, however, can generate information beyond simply confirming that details are consistent in various databases. It can yield new and previously unknown information about an individual not evident in either database. This form of data matching clearly is more privacy invasive if it collects information indirectly without the individual's knowledge and consent. All of this highlights the critical importance of greater transparency and control over data matching as well as rules to properly assess government matching proposals. These are noticeably absent in the existing data matching policy and should be expressed in law to provide appropriate guidance to government institutions.

Controlling information in public registers

The act's use and disclosure provisions do not apply to personal information that is "publicly available". What information can be considered "publicly available" has been the subject of heated debate since the act's very inception. Gradually two clear circumstances have emerged; the first when the individual gives express or implied consent for disclosure, and the second when information is required by law to be available for public inspection. The latter circumstance prompts the greatest privacy concerns.

The most common example of publicly available personal information is that held in a "government registry" (such as the Bankruptcy Registry or the Lobbyist Registry). Although there is a valid public interest in having the information available for inspection, few if any government registries control what details they disclose, the volume of records, or the uses that others can make of the information once disclosed. This has led to putting public registers on the Internet and bulk disclosures for marketing purposes. Arguably, government did not contemplate either use when they created the registers. Government institutions should never disclose personal information from a government registry for any purpose other than the one for which the registry was established. Nor should they disclose the registry's entire population or even make it available for inspection without specific

controls. Manitoba's *Freedom of Information and Protection of Privacy Act* is an example of the type of control we envisage. That act expressly prohibits the disclosure of personal information held by a government registry on a "volume or bulk basis." These and other rules on government registries should be included in the federal *Privacy Act.*

Expand mandate of the Privacy Commissioner

The Privacy Commissioner' ability to fulfil the ombudsman role has frequently been frustrated by limitations in the *Privacy Act.* For example, the Commissioner's role as a privacy advocate has been thwarted by his limited ability to seek Court review. As previously mentioned, the act only authorizes the Privacy Commissioner to ask the Court to review a complaint that access has been improperly denied. The law is silent on Court review of improper government collection, use, disclosure and disposal of Canadians' personal information. The act also does not expressly mandate the Privacy Commissioner to undertake research and prepare reports on privacy issues, nor to evaluate the privacy impact of legislation or new information management systems. And the Commissioner has no legislative mandate to educate the public about their informational privacy rights. While this silence has not prevented the Privacy Commissioner from pushing the limits when the public's privacy rights were at risk, without an express mandate there are no funds. This imposes such tight financial strictures that it hobbles the public's privacy ombudsman; these and other powers should be clearly stated in the legislation.

These are simply some of the principal recommendations we will ask Parliament to consider in amending the existing *Privacy Act.* Past efforts have been directed at fine-tuning specific provisions. Now nothing short of a major overhaul of the legislation is required. With the passage of the *Personal Information Protection and Electronics Documents Act* into law, amending the *Privacy Act* becomes a legislative imperative. The chance to revisit and rework a piece of legislation comes rarely in the life of a statute; it is all the more important to seize the opportunity and do what must be done to protect the privacy interests of future generations.

Counting Canadians—Keeping Promises, Building Trust

2001 Census—enhancing transparency in the census collection process

On May 15, 2001, Statistics Canada will ask some 31 million people in about 12.8 million households to complete and return their census questionnaires. Collecting the data will require 40,000 field staff, working from five regional offices. The total projected cost for the 2001 Census is $400 million.

The census is the federal government's largest collection of personal information and arguably its most detailed for the 20 per cent of Canadians who receive the long form. Naturally, Statistics Canada's conduct of the census interests the Privacy Commissioner.

As in previous censuses, 80 per cent of Canadian households receive the short questionnaire. The short form normally contains basic demographic questions, such as date of birth, sex, marital and common-law status and the relationship of persons living in the household. It could also include a question on the language first learned at home.

The remaining 20 per cent of Canadian households receive the long form. In 1996, in addition to the basic demographic data, the long form asked 47 additional questions on physical limitations, language knowledge, education, work and household activities, immigration, ethnicity and aboriginal status, housing, shelter costs and income. Some respondents consider many of these questions very intrusive, sensitive or even offensive.

Although Statistics Canada provides Canadians a good deal of information about the process of completing and returning their census forms, it does not

adequately inform Canadians that local census representatives in each community examine their completed questionnaires before sending them to Statistics Canada in Ottawa. Thus, respondents are not warned that someone they know could examine their completed form.

Of all the privacy complaints the Office received following the 1991 and 1996 censuses, those that generated the strongest negative reactions concerned respondents and census takers knowing each other. In most cases, complainants were both shocked and angry to learn that neighbours serving as census representatives reviewed their completed questionnaires; they assumed an unknown bureaucrat in Ottawa reviewed the information.

In summary, complainants felt the process had betrayed the promise of confidentiality and were outraged that friends, neighbours and others whom they know could have access to such financial information as the family members' income, mortgage payments, retirement savings and utility bills.

The great majority of complainants drew little comfort from Statistics Canada swearing census workers to secrecy or the possibility of fines and/or jail terms if they revealed personal information. Neither did much to remedy the resulting embarrassment and invasion of their privacy. Having their completed census forms reviewed by some unknown civil servant in Ottawa mitigated the intrusion to some extent. The Privacy Commissioner observed that allowing collection by neighbours who know the respondents demonstrates a complete lack of understanding of what privacy means.

To resolve the problems, Statistics Canada advised the Commissioner that it was developing a centralized edit methodology to replace the current system. Rather than returning completed questionnaires from an enumeration area to the local enumerator for editing and follow-up, all census questionnaires would be sent to district offices. Local enumerators would deal only with households that had not returned the form or with problems that district office staff could not resolve by telephone. In those cases, Statistics Canada could ensure that the assigned field enumerators were not local.

The "Centralized Edit System" was tested during the 1996 Census and again during the October 1998 "National Census Test" to prepare for the 2001 Census. Unfortunately, Statistics Canada found the tests did not yield the anticipated results. Centralized editing led to increased risks that respondents would not complete the forms, complete them only partially, and not return them. This caused more contacts with respondents than needed in the traditional method, increasing the risk of friction between census staff and respondents. This problem, combined with Statistics Canada's incomplete

and sometimes inaccurate household address file, convinced the agency not to use the centralized edit methodology for the 2001 Census.

Statistics Canada continues reviewing options for the 2001 census, such as computer-assisted telephone interviews in two regional offices, and collection over the Internet. Apparently the agency will test the Internet option on two Web sites during the next census. Respondents will be assigned a Personal Information Number (PIN) and their response data will be encrypted, thus eliminating the need to mail back census questionnaires to local census enumerators. Statistics Canada is also considering cutting the number of times census staff have to go back to respondents. In fact, the agency would like to reduce the rejection rate for the long questionnaires from 55 per cent to 35 per cent, significantly reducing the number of contacts with households and thus the friction between respondents and census staff.

Two tests will be conducted in the 2001 census and the results compared; one using a sample of 125,000 long questionnaires (approximately 5 per cent) for which there will be no edit and no follow-up, and the other using a sample of 325,000 long questionnaires (approximately 14 per cent) involving only telephone follow-up.

Statistics Canada will also assign census takers in urban areas to neighborhoods outside their own, thus reducing the risks of their collecting information about someone they know. This requirement will be considered when the agency hires staff for the next census. However, in rural areas and small towns it is not possible to guarantee that respondents and census representatives will not know one another; the pool of available staff is not large enough to avoid the situation. In addition, Statistics Canada finds that the only way to ensure all households are enumerated in rural areas is by assigning someone thoroughly familiar with the area.

However, Statistics Canada will attempt to alleviate the problem with several steps. It will print on the back of both the questionnaire package and the return envelope an advisory that a "Statistics Canada representative responsible for your area" will review the questionnaires. Respondents who object to providing their completed census form to their local enumerator will be told by the enumerator or the Census Help Line that they can have a census commissioner collect the information or they can mail their completed form to the regional office. The agency will also provide census

staff additional training and procedures to emphasize the importance of protecting collected information and heighten census enumerators' awareness of privacy concerns.

Although these steps might address some aspects of the problem, they do not resolve it. The Commissioner is concerned that the process lacks transparency. For example, the proposed message on envelopes advising that an agency official will review their questionnaire, does not alert respondents to the possibility that it might be someone they know—a neighbour or friend.

Since Statistics Canada recognizes that it is not uncommon for residents in a collection area to know the enumerator (and particularly true in rural areas), it must clearly inform respondents about the probability and offer them options for returning the questionnaire. And these measures should apply to both the short and the long questionnaires because the short form will ask a question on sexual orientation (same-sex partner). The Office suggested wording to include in both the census guide and on the front of both census forms that would meet the transparency requirement:

> Although Statistics Canada is taking measures to avoid having census enumerators work in areas close to where they live and/or to ensure that enumerators do not know any of the respondents in their collection area, residents in a collection area might know their local enumerator. If you are personally acquainted with the local enumerator and feel uncomfortable giving information to this person, please call our 1(800) Census Help Line to find out about the alternate arrangements for returning your completed questionnaire without having the local enumerator see it.

The Office also believes that part of the problem could be avoided by clearly instructing census representatives to actively offer alternate arrangements when they know the householder. It is best to offer this option at the outset rather than waiting to have the respondent object. Census representatives must also be instructed to turn over the completed questionnaires of anyone they know to the area census commissioner.

Historical census records

Last year we reported on the debate over releasing post-1901 census returns. All censuses in Canada since 1901 have been the subject of a repeated promise—set out first in regulation, then in legislation—that individual

returns would not be disclosed to anyone outside Statistics Canada. As a result, Statistics Canada is legally prohibited from releasing the completed census forms to the National Archives. This has angered historians and genealogists seeking access to the information, and they have publicly called for retroactive changes to the law.

Any government promise of confidentiality is serious enough, but the one protecting the census is particularly important. Census questions demand personal information. The information gathered through 20th century censuses became steadily more intrusive, but even early in the 1900s some questions—about, for example, education, religion, nationality, race, occupation, and earnings—were intrusive. And the answers revealed information that people would not necessarily choose to make public. Canadians are required to answer census questionnaires and the maximum penalties for failing to comply are severe: fines and imprisonment. Keeping the information confidential, using the information for statistical purposes only and not releasing it in identifiable form are arguably the trade-offs that bolster public acceptance of censuses, and compliance with the law.

Despite the clear prohibition on release of the material, the Minister of Industry last year asked Statistics Canada to look at ways in which the legislation might be amended to allow access to individual census returns. Statistics Canada proposed two options: amending the *Statistics Act* to allow access to the 2001 and all subsequent censuses; or amending the act retroactively to override the confidentiality provisions. The Privacy Commissioner opposed both options; the first because the absence of guaranteed confidentiality risked compromising the census process, and the second because it would break the legal promise Parliament made to Canadians.

The Minister's response was to set up an expert panel to examine the issues and make recommendations. The Commissioner appeared before the panel in February 2000.

The Commissioner urged the panel to recognize the important social issues of privacy and governance the debate has raised. He pointed out that the question is not whether a "personal" or "individual" interest in privacy should cede to a "public" or "societal" interest in genealogical and historical research. The historians and genealogists who want access to the census materials do not have an exclusive claim to represent the public interest or express a public right. Privacy is also a public right, upon which rest the freedoms and mutual respect fundamental to Canadian society. What was facing the panel was more than a decision about the privacy of the

respondents to the 1906 or 1911 census. Its decision will have implications for their privacy certainly, but it will also have an impact on the privacy of all Canadians.

A number of important privacy issues are at stake. Most critical is the principle, found in all data protection laws and codes, that personal information should not be used for purposes unrelated to those for which it was collected. Any such unrelated use should depend on the consent of the person who gave up the information.

Another issue is the problem of keeping personal information longer than required for its stated and intended use. The very existence of these records, long after their legitimate statistical function has been fulfilled, is an invitation to unrelated uses. This is a typical example of what privacy advocates call "function creep", and highlights the importance of establishing and respecting limits on retention of information.

Finally, there is the question of when an individual's privacy rights can be considered extinguished. Some suggest that the privacy rights of those who completed the 1906 and 1911 census returns have somehow vanished. Even assuming that all are dead (which is not necessarily true), this proposition is not self-evident. As a matter of general principle, society recognizes that some rights continue after death; this is the basis on which people are allowed and even encouraged to dictate in their wills how their property is to be distributed after their death. The *Privacy Act* itself recognizes that information remains "personal" for 20 years after the death of the person concerned.

The Commissioner stressed that any proposal to amend the law retroactively should be approached with great caution, lest the result diminish confidence in government promises—not just in specific agencies, but also in government that professes to rule with the consent of the governed. Proponents have presented a retroactive amendment as though it were innocuous. The promise of confidentiality has been described as "a legal technicality in an outdated piece of legislation." The Commissioner, however, reminded the panel that the promise of confidentiality was fundamental to the process of obtaining answers to census questions.

Canadians have never been particularly comfortable about the intrusiveness of census questions. The number of inquiries and complaints to the Privacy Commissioner over the years is one indicator of this discomfort. Yet Canada's census response rate is high. Despite the intrusiveness of the questions, the sensitivity of the answers, and their unease with the process,

Canadians agree to participate.

Part of the reason is that they are coerced. Intrusive questions were, and are, backed by the threat of fines or imprisonment. But governance in Canada does not rest primarily on coercion. Indeed, as generations of Canadian schoolchildren have been encouraged to appreciate, one of the principal points of pride in Canadian society is responsible government that rules with the consent of the governed. At the heart of the census process was not the threat of force but an agreement between government and governed: that intrusive questions would be answered, but that the answers would be protected. To abrogate the promise retroactively risks trivializing that agreement, and all such agreements.

The Commissioner also recommended that, if the panel chose not to support the government's promises and Canadians' privacy rights, at the very least it should consider a compromise that would mitigate the impact on privacy and governance. Recognizing that the census returns are of particular interest to historians and genealogists because they are one of the few sources of documentation about Canadians in the early 20th century, the Commissioner suggested determining a date after which genealogists' and historians' objectives could be met without having access to the census materials. Census returns dating before the cut-off could be released to the National Archives. All census returns after that date would be destroyed, once they fulfil their legitimate statistical use.

The Commissioner also urged the panel to consider whether "tombstone" data—names, ages, addresses—could be isolated from the more intrusive details, on the principle that government should first try the least intrusive measure that would achieve the objectives and resort to more intrusive measures only when genuinely required.

If Parliament amends the *Statistics Act* to remove confidentiality, the process must be transparent. Statistics Canada must advise Canadians when it conducts the census that it will eventually release the information. If, as Statistics Canada says, confidentiality is one of its most effective ways of securing willing cooperation, then Parliament must find some other way of convincing Canadians to cooperate. The Commissioner also urged the panel to consider Australia's model, which will allow respondents to the 2001 census to choose (by opting in) to have their returns stored and released after 99 years. (Australia currently destroys its census returns.)

Finally, the Commissioner observed that retroactive change to the agreement between government and governed undoes the conditions under which

Canadians participated in the census. Such a change must be the subject of full Parliamentary debate, with every MP required to consider it and be held publicly accountable.

The Commissioner's brief, "The census returns, privacy, and questions of governance," is available from our Office and on our website.

SIN, Again

Some issues never go away. Looking back on past annual reports, SIN stories have been a recurring feature. This year's edition continues the tradition with two stories. The first deals with Human Resources Development Canada's (HRDC) proposals to improve its management of the number following the Auditor General's critical report.

That report, discussed in last year's annual report, raised several concerns, not least of which was the extensive use of the SIN as a widespread identifier. Past efforts to control the SIN have included several private members' bills, one by then-MP Perrin Beatty in 1979. In 1987 a Parliamentary committee recommended rigorous controls following its three-year review of the *Privacy Act*. Government acted on neither although it did introduce a policy limiting federal government use of the number. Now twenty years after Mr.Beatty first proposed legislative restrictions, government continues studying ways to control private sector use of SIN. To borrow one of the popular marketing slogans of our time, our advice is "Just do it".

The second article deals with a New Brunswick pilot project that was intended to improve HRDC's administration of the SIN, another longstanding issue, by speeding up issuance of SINs and improving the process of verifying the information required to obtain a SIN.

The HRDC Position Paper

One result of the Auditor General's review was Parliament's tasking the Standing Committee on Human Resources Development and the Status of Persons with Disabilities (the Standing Committee) with studying the administration and policy regime governing the SIN. The Standing Committee's report, *Beyond the Numbers: The Future of the Social Insurance Number System in Canada*, recommended legislation to establish legal uses of SIN and penalties for misuse. The report also recommended that HRDC prepare a position paper assessing various options for addressing long standing administrative problems with the management of the SIN, as well as the privacy concerns.

HRDC tabled its position paper, *A Commitment to Improvement: The Government of Canada's Social Insurance Number Policy*, before Parliament on December 7,

1999. The paper considered three policy options: 1) transforming the SIN into a national common client identifier supported by biometrics technology; 2) drafting specific legislation to limit who may use SINs and for what purposes, and introducing administrative reforms to improve its management; and 3) amending existing legislation to improve SIN management, complemented by the safeguards in Bill C-6 against private sector abuse of personal data such as the SIN.

The position paper rejected transforming the SIN into a national common client identifier, in part because the costs would be prohibitive. The government estimated the costs for issuing high tech cards supported by biometric technology at $1.1 billion to $3.6 billion. The government also acknowledged that establishing a comprehensive national system of identification would carry with it "severe privacy concerns". But HRDC's paper also rejected legal restrictions on SIN use, thus dismissing one of the Standing Committee's key recommendations. HRDC rejected this option arguing it "would almost certainly lead to increased financial costs to business due to a generally less reliable credit checking system".

HRDC suggests that it can deal largely with its SIN management problems under current legislation, except for certain limited amendments to the *Employment Insurance Act*. The department is also relying on Bill C-6 to resolve recurring concerns about the private sector's uncontrolled use and abuse of the SIN. It expects to improve its management of the SIN by reducing the number of documents accepted as proof of identity for new SIN applicants, and increasing its access to sources such as provincial vital statistic registries to verify identity (see the New Brunswick project below).

In order to detect and prevent fraudulent use of the SIN, the position paper also describes measures to expand users' access to the Social Insurance Register. This would allow certain provincial authorities, and potentially even private companies, using the SIN to verify a number's authenticity and the identity of its rightful owner. In addition to basic identifying data, users could also obtain information about the status of the SIN; for example, that the individual is dead or the account has been cancelled, has been inactive for 5 years, or is under investigation. Access to this information would alert users to possible problems or irregularities associated with the number.

HRDC also recommends amending the *Employment Insurance Act* to help detect and deter fraud. Those amendments would both expand the range of SIN-related offences subject to administrative sanctions and increase the severity of those sanctions. Among the offences are 1) illegally using the SIN to claim employment insurance benefits; 2) illegally using the SIN in

connection with another federal, provincial or municipal department or agency; and 3) illegally using a SIN in dealings with the private sector. Penalties for these offences would range from $400 to $1,200.

We are immensely relieved that the government rejected the proposal to introduce a national system of citizen identification, an idea that we have long opposed. Nevertheless, we are disappointed that HRDC rejected the Standing Committee's recommendation to set out in law who may use the SIN and for what purposes. Any legislative regime that permits both federal and provincial governments to use SINs for any purpose, coupled with expanded access to the SIN Register for client identification, risks transforming the SIN into the very thing the government said it should not become—a de facto national common client identifier.

We can appreciate in principle HRDC's rationale for collecting and storing certain information about the status of a SIN, and for sharing the information with authorized users. But the initiative poses significant privacy risks if not strictly regulated. The register currently collects and discloses limited information; the government position paper opens the door for expansion.

"I'M AFRAID YOUR VITAL FINANCIAL SIGNS ARE TOO WEAK TO OPERATE."

These risks inherent in the current permissive legislation further justify enacting specific legislation governing the SIN. HRDC rejected this option, however, arguing that it would force the private sector to incur unacceptable financial costs and risks if it were denied the right to collect and use the SIN for its own purposes. It will rely on Bill C-6 to prevent any abuse of the SIN in the private sector.

The claim of undue hardship on the private sector is, frankly, unsubstantiated. HRDC had promised to survey private organizations concerning their use and misuse of the SIN but it did not do so before preparing its position paper. HRDC, in conjunction with Statistics Canada, is now preparing to conduct such a survey.

We hope that this survey will shed some light on the ability of Bill C-6 to deal with all the abuses of the SIN in the private sector. Although the legislation will require private organizations to obtain individuals' consent for any use of their SIN, those are uses the SIN was never intended to serve. Allowing private sector convenience to override legitimate legal protection for Canadians' social program and tax number is putting the cart before the horse.

If many different businesses use the SIN as a common file identifier, the scope for covert data linkages increases dramatically because the SIN, along with other personal account numbers, can be used as a kind of access key whose mere possession can be construed as authorizing a data transfer or linkage. This risk is made all the more serious by the principle of "implied consent" which Bill C-6 expressly recognizes. Other foreign personal data protection laws—notably those of Hong Kong, Australia and New Zealand—expressly limit the right of private organizations to use personal and file identifiers assigned by other organizations. With no such prohibition in Bill C-6, there is a compelling case for legal restrictions on SIN.

We commend HRDC's proposal to expand the list of offences that will incur administrative sanctions; however, we question whether the penalties are a sufficient deterrent. Identity theft is an expanding and increasingly profitable crime; there are substantial gains to be made from misusing the SIN and other identifiers. In our view, the penalties for abuse of the SIN should be proportional to the potential harm that innocent people may suffer from its illegal use. The present proposals fall far short.

New Brunswick SIN Tele-App Pilot Project

The New Brunswick Pilot Project was a partnership between HRDC and New Brunswick's Vital Statistics branch conducted between April and October 1998. During that period, native New Brunswickers could apply for a SIN by telephone using Integrated Voice Response (IVR) technology and an HRDC agent. HRDC would then verify the applicant's identity on-line with the provincial birth, marriage, change-of-name and death registries. Once the information was verified, the HRDC agent could approve the application, create a new record in the Social Insurance Register database and issue the applicant a new SIN over the telephone. A SIN card would follow in five to seven days.

Early in September 1999, HRDC gave the Office its evaluation report on the pilot project for review and comments. We assessed whether using provincial vital statistics data to validate SIN applicants' information complied with the fair information principles of the *Privacy Act*. These principles essentially

define how and when personal information may be collected, kept, used, disclosed to third parties, and finally destroyed.

We concluded that the *Employment Insurance Act* and the *Canada Pension Plan Act* gave HRDC the legal authority to collect all the information needed to identify accurately individuals who apply for a SIN, a replacement card, or to amend their social insurance register records. We also determined that the New Brunswick *Vital Statistics Act* allowed HRDC access to selected personal information to register New Brunswick-born applicants for SINs, and to ensure the information applicants provided was accurate.

HRDC's access to the registries was limited to selected data elements related to births, marriages, deaths and changes of name that it clearly required to verify a telephone applicant's identity. Although collecting this personal information appeared to be directly related to, and necessary for, the operation of lawful HRDC programs, we were concerned about it collecting information from the province's marriage registry. While it is acceptable for HRDC to use marital information to authenticate the applicant's identity, HRDC should not record this information in the SIN Register unless the applicant's name changed as a result of marriage.

HRDC also reported that more than 500 SIN applications were rejected for various reasons during the pilot project. What happened to the information (for example, birth registration or credit card numbers) submitted by applicants who were subsequently rejected, or who changed their minds and discontinued the calls? Did HRDC keep the information?

The Office also looked at the transparency of the process for applicants. We found the system provided callers clear instructions on how to apply for the card. They were informed about the information required, how the information would be used, and who would have access to it. They could exit the system at any point. By staying on the line and entering the requested information on the telephone keypad, applicants were effectively authorizing HRDC to proceed with their application. However, we believe that HRDC should make it clear in its instructions that callers are consenting when they enter the information.

Although vital statistics records can be a valuable source to verify data for the SIN registration system, this use may have privacy implications for provincial vital statistics agencies. Traditionally, birth, marriage and death records are created for civil registration, providing birth, marriage and death certificates, and compiling vital statistics. Any disclosures for administrative purposes beyond those the province gave when it collected the information,

could violate provincial fair information codes. These codes, like the *Privacy Act*, require that personal information be used only for the purpose for which it was obtained. Any departures from the principles need justifying on strong public interest grounds.

Provincial vital statistics agencies will have to answer this question if HRDC seeks to expand its project to other provinces and territories. They will also have to consider whether they have the necessary legal framework in place to allow HRDC on-line access to vital statistics registries for its SIN registration program.

But there are more than privacy and legal implications; sharing or linking vital statistics data between provincial and territorial vital statistics agencies and HRDC raises concerns about confidentiality and security. Organizations that link data must have all the necessary safeguards in place to ensure that only authorized staff have access at the right time for the right purpose. Thus, if HRDC decides to expand its SIN Tele-App project to other provinces, not only will it have to deal with the problem of potentially incompatible operating systems, it will also have to ensure the confidentiality and security of the data. Although we did not receive all the technical details of the New Brunswick system, it did appear to have the requisite controls in place to ensure the confidentiality and the security of all the information being exchanged.

At the end of the pilot project in October 1998, New Brunswick Vital Statistics agreed to store on HRDC servers all of its information required to process a SIN application. This arrangement fails two privacy tests: HRDC is effectively collecting information about everyone on the vital statistics registers, including those who have not yet applied or who may never apply for a SIN. Thus it is collecting far more information than it needs and violating the collection principle of the *Privacy Act*. Such a blanket collection also fails to respect another fundamental privacy principle—consent. Federal institution are required, wherever possible, to obtain individuals' consent before collecting their information from another source.

We also learned that HRDC has continued access to the New Brunswick registries when processing mailed applications from those born in the province. We do not know whether these applicants were clearly informed at the time that their information would be cross-checked with the provincial vital statistics databases. HRDC is responsible for telling these applicants how their data will be used; failure to do so would contravene the principle that government must inform individuals why information is needed and how it will be used.

Our comments were submitted to the standing committee and HRDC in early December 1999. In late February 2000, we met with HRDC representatives to discuss our comments.

As a result of the meeting, the HRDC representatives agreed to work on a solution to inform the public that any names formerly used, for example a married name, will be maintained in the SIN Register. They also agreed to consider the suggestions that the agreement between HRDC and the Government of New Brunswick to store all the provincial vital statistics information on a HRDC server clearly reflects the fact that the information is used only for the intended purpose of registering individuals for a SIN, and that ownership of the information belongs to the province. HRDC agreed to modify the paper application and the telephone message on the SIN Tele-App system to ensure that the public is informed about the use HRDC makes of the information that is made available by Vital Statistics.

HRDC participants explained that, in the cases where it was necessary to reject a SIN application through the SIN Tele-App process, the information was deleted from the records and no information was retained. In the case of the paper application process the information is maintained in a separate file for a six-month period pending the resubmission of the application from the applicant. HRDC will identify a method that will be used in both the SIN Tele-App and the paper application process to inform the general public that in cases where it is necessary to reject an application, the applicant's information will be retained on file for a period of six months, and will be used to process the application when resubmitted.

Finally, HRDC has assured us that the Office will be kept abreast of any future developments as the department moves ahead with a national roll out of the SIN Tele-App service.

A Citizen Profile in all but Name—HRDC's Longitudinal Labour Force File

The audit

Two years ago the Office concentrated its meagre compliance resources (four staff) almost entirely on Human Resources Development Canada (HRDC). Why?

The choice was fairly obvious. With federal government reorganization, HRDC became a virtual behemoth—the federal government's largest repository of personal information on its citizens. The department absorbed labour market adjustment programs from the former Labour Canada, social and income security programs from the former Health and Welfare Canada, social development and education programs from Secretary of State, and Unemployment Insurance and labour market programs from Employment and Immigration Canada and the Canada Employment Insurance Commission.

The department is tasked with providing a safe, healthy and stable work environment, administering income security programs, and helping individual Canadians find and keep work. The result is a huge clientele and workload, a budget to match, and a comprehensive collection of personal data on virtually everyone in the country—all of which combine to exert intense pressures on HRDC to ensure its programs are delivering the goods, and to tighten and fine tune the systems to eliminate fraud.

HRDC depends heavily on information technology to deliver, monitor and assess programs and services—indeed, given the workload and staff cuts, the department could likely not function without it. The department is also a natural candidate for devising new applications for technology. But the combination of huge personal databases, powerful computer systems and growing links with provincial social programs and the private sector as the federal government downloads service delivery, makes HRDC a natural focus for privacy concerns.

The audit team concentrated on an informal but systematic review from

which it assembled a profile of the department. We identified the information collected and the purpose, followed its flow through HRDC, and identified the subsidiary uses and sharing of the data and its retention standards. From there the team concentrated its resources on those activities that seemed to put clients' privacy most at risk. Two of these stood out; the Common Client Identifier project and the Longitudinal Labour Force File.

The Longitudinal Labour Force File

Successive Privacy Commissioners have assured Canadians that there was no single federal government file, or profile about them. We were wrong—or not right enough for comfort.

Not having a single client file is a good thing—on the principle that the more separate the databases, the lower the risk of indiscriminate collection, unrelated uses and improper disclosures of personal data. Organizing information into "silos"—discrete collections—may be less "efficient" but more protective of individual privacy, as each silo holds only information required for a particular purpose. Only Statistics Canada gathers comprehensive information about individuals but does so only for statistical purposes, not to make decisions about them. And Statistics Canada's data is stringently protected; abusers can be fined and jailed.

HRDC's Strategic Policy Branch developed the Longitudinal Labour Force File for research, evaluation, policy and program analysis to support departmental programs and services.

The Longitudinal Labour Force File is the next thing to a citizen profile. The research database contains records on more than 33.7 million individuals—at last count—drawn from widely separate internal and external government files and time periods. The data is never purged, which explains why there are more records than the entire population of Canada.

The Data Development & Technical Services group in the Strategic Policy Branch extracts data gathered from other federal departments and other levels of government using personal identifiers. The group updates the databases frequently to ensure the information is as current as possible and reflects changes to legislation and operational procedures. The data is drawn from files in several programs, including

- T1-Income Tax Returns and T4-S and T4-F forms issued for income tax purposes;
- Child Tax Benefits;

- Immigration and Visitors files (from EIC – 1993 or earlier);
- Provincial and municipal welfare files;
- National Training Program;
- Canadian Job Strategy;
- National Employment Services;
- Employment Insurance Administrative;
- Record of Employment, and
- Social Insurance Master file.

And there are proposals to expand the database to include data on social assistance recipients from additional provinces and territories, as well as data from the Canada Student Loan Program, the Canada Pension Plan and the Old Age Security Program.

A de facto citizen profile

Following the audit, the Commissioner wrote to HRDC setting out his profound concerns about what amounts to a comprehensive, permanent and to all intents, invisible citizen profile. A steady exchange of letters and telephone calls ensued.

Gathering some data for research is not necessarily a privacy intrusion. Many government databases may be used for research, and the *Privacy Act* specifically allows research disclosures. What, then, is the problem with the Longitudinal Labour Force File?

There are several. First, its comprehensiveness; this is an extraordinarily detailed database, which could contain as many as 2000 elements on an individual including education, marital/family status, language, citizenship and landed immigrant status, ethnic origin, mobility, disabilities, income tax data, employment histories, labour market activities, use of social assistance and Employment Insurance. Continually centralizing and integrating so much personal data on almost every person in Canada poses significant risks to our privacy.

Second, the database is relatively invisible. HRDC is not trying to hide its existence. In fact, it describes the database in *Info Source* and on its Web site. Unfortunately, neither are widely read, nor easily understood, and the description of the database contains few details. Canadians don't know how much information is being collected about them or the extent to which it is

being integrated and shared with others. For example, how many taxpayers know their financial information is in an HRDC profile? HRDC can provide the data to private sector research firms under contract for planning, statistics, research and evaluation. It can give the data to non-government organizations (such as academic researchers and universities) to carry out studies on HRDC's behalf under a formal agreement or contractual arrangement. Some of the information may also be used by government organizations (e.g. Statistics Canada, provincial and territorial governments) to conduct research into the labour force, the labour market and other related fields.

Third, its permanence; this database is never purged. The database captures information from the cradle to the grave and beyond. Research databases should have defined parameters that include a limited storage time. Without an end, the temptation is to subject everyone to unrelenting information surveillance. This database needs limits.

Fourth, there is no legal protective framework. The government's pre-eminent statistical agency, Statistics Canada, operates under very strict legislation—complete with penalties—to protect the personal data it gathers for research and statistics. It cannot share, sell, or use this information for operational purposes. No such walls protect the HRDC research databases.

Compiling such comprehensive longitudinal records by record linkage or matching is a hazard to informational privacy because of the temptation for government to use the information for data mining and individual profiling. A so-called "research database" may soon lend itself to other purposes, raising fears that data could be used to make decisions or predictions about individuals, or could be retrieved in unforeseen ways—by disabilities or ethnic origin, for example—to the detriment of individual rights. This fear is not unfounded; about two years ago HRDC launched a pilot project—the Service Outcome Measurement System—to use research data for program administration. The pilot was put on hold while the department focused on Y2K projects.

We first alerted HRDC to our serious concerns about the Longitudinal Labour Force File in September 1998, and repeatedly since. In summary, the Commissioner urged the department to

- Establish a fixed retention span for data in the Long File;
- Introduce penalties and sanctions for misuse of the information;
- Ensure that research data not be used for program administration;

- Establish strict controls and data protection safeguards on its collection, use and retention of any personal information used for research and evaluation; and
- Incorporate in its enabling legislation a clear purpose-specific research mandate.

HRDC's response
HRDC conducted its own internal review focussing on the size of the database, its indirect method of collection, notification of individuals about secondary uses and its permanent retention of the data. In September 1999, HRDC provided us a copy of the report.

The size of the database: HRDC considers all the data vital to help it develop policy, manage the effectiveness of its "interventions" and improve programs and service delivery. It rejects the observation that the collection seems speculative but—tellingly—observes, "from a pure business perspective, it would not be effective for HRDC to collect and maintain information that is not useful." The department argues that a credible evaluation of the "labour market and social policy analysis must take account of a daunting array of factors", and this information must be "disaggregated" to identify target specific groups and areas and to assess impacts on groups and individuals. The department also observes that all the information relates to its own operating programs or can be disclosed by other departments under their own legislation and therefore is permissible under the Privacy Act.

Indirect collection: The department argues that it is required to collect the information directly from the individual only when it intends to use it for an administrative purpose; that is, to make a decision directly affecting the person. Since the Long File is not used for that purpose, direct collection is not required. HRDC also maintains that since the *Privacy Act* only requires direct collection "whenever possible", Parliament has specifically authorized indirect collection in circumstances such as this when, as HRDC maintains, "it would not be possible to obtain the information directly from the individual...". Finally it observes that departments may disclose information under section 8(2) which includes a disclosure for research.

Clear notification: HRDC argues that it does not need to inform individuals about its indirect collection because the *Privacy Act* requires federal institutions to "inform the person from whom they collect personal information". Since it collects individuals' information from another organization, and since it will make no decisions about the person based on

the Long File, HRDC maintains it need not notify the individuals. However, the department undertook to review its description in *Info Source* of the content and use of the database.

Unlimited retention: The department rejected this concern, arguing it needs to analyse the data through different market cycles and to assess the impact of such variables as free trade, technological change and market globalization. It also observed that the *Privacy Act* does not speak about retention limits on research databases.

No protective framework: HRDC argues that existing legislation and internal policies provide adequate protection of personal information. Personal data is masked and access to unmasked data is limited. However, it concedes that there are fewer penalties for those who misuse information than in the *Statistics Act* and the *Income Tax Act*. Nevertheless, the department believes its staff professionalism and internal policies are sufficient.

HRDC concluded that it "respects all the privacy legislation as well as related legislation and associated rules".

Since then, the department has agreed to limit the retention span of the information to 25 years, tighten access to the data and introduce measures to prevent administrative use of the information. HRDC is also considering amendments to its legislation to provide penalties and sanctions for misusing the information.

The privacy position: The Commissioner commended HRDC for the moves but underlined that most of its actions focus on protecting security, not privacy. He wrote, "...it is very difficult for me to accept, for example, on the basis of your review, that all of the information contained in the Longitudinal Labour Force File is indeed directly relevant and necessary to HRDC's operating program and policy activities." And in a later letter he observed, "...I still view the Longitudinal Labour Force File as something tantamount to a citizen profile."

He also took issue with the department's assertions that it is in compliance with the *Privacy Act*. "...One does not have to be a privacy expert to see that this assertion rests on a restrictive and literal interpretation of...the fundamental rights that are at the heart of the *Privacy Act*...I do not find it satisfactory that the federal government's largest department defends the creation, maintenance and expansion of dossiers on vast numbers of Canadians by saying that it meets minimum legal provisions", the Commissioner observed. "Surely a higher duty than that is imposed."

True compliance with the law, and true accountability to citizens, would require complete transparency in HRDC's research operations and decision making. And it demands that Canadians know why their information is being collected, how it will be used, how long it will kept, and to whom it will be disclosed. The department's response is inadequate. HRDC has offered to continue the discussions and we are happy to oblige. This is a difficult time for HRDC and we do not want to be seen as piling on. But it is now more than two years since this discussion began. It is time to open it to include all those whose information the department is systematically mining in the interests of "social policy development".

On the Hill

To better protect Canadians' privacy, the Privacy Commissioner's Office attempts to keep abreast of new legislation, reviewing each bill for privacy implications (which are not always obvious). If a bill could have substantial privacy impacts, the Commissioner makes a written or oral submission to the appropriate committees. In so doing, the Commissioner fulfils his role as Parliament's privacy watchdog, informing elected officials and recommending ways to either avoid or minimize the privacy intrusions.

New bills

Recent government bills with privacy implications include:

- Bill S-10, amending the *National Defence Act*, the *DNA Identification Act* and the *Criminal Code*. This bill would bring offenders from the Canadian military under the ambit of the national forensic DNA database created by the 1998 *DNA Identification Act*. The act currently applies only to civilian offenders. The bill contains two welcome proposals: one restricts the use of genetic samples and profiles to law enforcement, the other requires the Royal Canadian Mounted Police Commissioner to report annually to the Solicitor General on its operation of the national DNA database. However, the Privacy Commissioner restated his concerns to the Senate Standing Committee on Legal and Constitutional Affairs over the number of offences for which a judge may order a genetic sample. The Privacy Commissioner continues to believe that genetic samples should be taken from an offender only after s/he is convicted of a violent offence, and only if that offender is likely to re-offend and in so doing leave behind a genetic sample.
- The *Proceeds of Crime (Money Laundering) Act* (Bill C-22, formerly Bill C-81) would establish specific measures to detect and deter money laundering and facilitate prosecution of money laundering offences. It would require financial institutions to report suspicious transactions, and it creates a Financial Transactions and Reports Analysis Centre of Canada to filter the reports and alert the appropriate police force or the Canada Customs and Revenue Agency to any suspicious transactions. The Centre would be subject to the provisions of the *Privacy Act*. In last year's annual report (pp 31-34), the Privacy Commissioner observed that the bill could conflict with both the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. The Commissioner also has concerns about the definition of a "suspicious transaction" and the nature of the centre. This bill is discussed in more detail below.

- The *Youth Criminal Justice Act* (Bill C-3, formerly Bill C-68) would modernize the current *Young Offenders Act*. The provisions of greatest concern to the Office deal with proposed disclosures of young offender information to victims and the public, and forensic analysis of genetic samples from young offenders. These new provisions could decrease the privacy provided young offenders under the current legislation.

Other government bills with privacy implications include:

- The *Canada Elections Act* (Bill C-2, formerly Bill C-83). This bill modernizes the *Elections Act* and contains provisions dealing with the National Register of Electors. Members of the Standing House Committee on Procedure and House Affairs approved an amendment allowing Elections Canada to collect voters' telephone numbers (where not confidential) and include them on electoral lists. The Privacy Commissioner asked committee members to reconsider their decision, and recommended that the Chief Electoral Officer be required to notify voters that political parties use the personal information on voters' lists for fundraising and party membership solicitations.
- The *Canadian Institutes of Health Research Act* (Bill C-13) would establish virtual health research "institutes" (*i.e.*, groups of researchers with no shared physical work environment) that would create new knowledge and translate it into improved health and a better health care system for Canadians. The Office is concerned about the real possibility that these researchers will gain access to vast amounts of personal information without individuals' knowledge or consent.
- The *Citizenship of Canada Act* (Bill C-16) would modernize the existing *Citizenship Act*. It would codify the Minister of Citizenship and Immigration's practice of disclosing names and addresses of new citizens to Senators and Members of the House of Commons for congratulatory letters. At present, the Minister must first seek new citizens' permission to do so (by opting in). Bill C-16 makes disclosure the norm, placing the onus on the citizen to opt out. Opting out is both poor privacy practice and reminiscent of such marketing strategies as the cable companies' negative option billing which so offended subscribers. The Privacy Commissioner of Canada wrote to the Minister of Citizenship and Immigration explaining this concern.
- The *Nisga'a Final Agreement Act* (Bill C-9) would implement the recent self-government agreement between the federal government and the Nisga'a First Nation, and would add aboriginal governments to the list of organizations to which a federal agency may disclose personal information without the prior consent of the individuals concerned.

New Legislation

The following government bills became law over the past year:

- Bill C-7 (formerly Bill C-69) amended the *Criminal Code* to allow pardon records of former sex offenders (previously sealed) to be flagged in the Canadian Police Information Centre (CPIC) database. This allows the RCMP to disclose the records if the offender is screened for a position of trust with children or other vulnerable groups. (The CPIC database is shared by most law enforcement agencies in Canada and is maintained by the RCMP.) The Senate passed this bill in December 1999.
- Bill C-43 replaced Revenue Canada with a new Canada Customs and Revenue Agency. The main privacy implications of this bill dealt with the huge databases of taxpayer's information that have become the responsibility of the new agency. The new agency is subject to the provisions of the *Privacy Act*. This bill received Royal Assent in April 1999, and came into force in November 1999.
- Bill C-67, dealing with foreign financial institutions operating in Canada, includes provisions on their use and sharing of customer information and on tied selling practices. This bill received Royal Assent in June 1999.
- Bill C-71, implementing the 1999 federal budget, included provisions for sharing taxpayers' information for worker's compensation purposes. This bill received Royal Assent in June 1999.
- Bill S-22 implemented U.S. Customs' officers' pre-clearance of travellers entering the United States of America through Canada. The two main privacy implications of this bill concerned the protection afforded on Canadian soil by such Canadian laws as the *Privacy Act*, and U.S. officials' collection and use of detailed behavioural profiles of travellers. These concerns were outlined in the Privacy Commissioner's 1998-99 annual report (pages 36-38). The bill received Royal Assent in June 1999.
- The *Civil International Space Station Agreement Implementation Act* (Bill C-4, formerly Bill C-85) implements the recent international agreement on developing and operating a civil space station, and contains provisions dealing with the international sharing of information for law enforcement purposes. The bill was given Royal Assent in December 1999.

Private members' bills and motions

Of course, new legislation does not consist solely of government bills tabled by ministers of the Crown. Members of Parliament and Senators may also table their own private bills through a sort of legislative lottery. This past year has seen an unusual flurry of private bills and motions with privacy implications, among them:

- Bill C-270 (MP Jim Pankiw) would forbid the publication of the identity of a person facing charges before the first finding of guilt or innocence by a court.
- Bill C-393 (MP Mac Harb) recommends that federally regulated financial institutions, federally incorporated corporations and credit bureaux advise consumers before giving any information on their financial history to a credit grantor or credit bureau. The bill also offers consumers a complaint procedure through the Superintendent of Financial Institutions.
- Bill C-395 (MP Mac Harb) would restrict the use of social insurance numbers to agencies or organizations lawfully authorized to collect the numbers.
- Bill C-417 (MP Greg Thompson) would, among other things, give patients a right of access to, correction and control of their health records.
- Bill C-419 (MP Bill Gilmour) would allow persons not wanting to receive telemarketing calls or faxes to include their telephone number on a list maintained by the Canadian Radio-Television and Telecommunications Commission. Telemarketers who do not respect this list would commit an offence and be liable to substantial fines.

And echoing the Privacy Commissioner's call for long-needed amendments to the *Privacy Act* (summarized in another section of this annual report), Motion M-19 (MP Mike Scott) called for a House of Commons committee to table a bill remedying the weaknesses of the *Privacy Act*. The proposed remedies would have included relief or compensation for those who suffer as a result of improper disclosure of their private information, and penalties for those who wilfully violate the act. Unfortunately, the motion was dropped from the Order Paper after a short debate.

Not all private bills tabled this year were so pro-privacy, however, such as those dealing with law enforcement matters. MPs Myron Thompson (Bill C-234) and Chuck Strahl (Bill C-244) both tabled bills that would empower law enforcement officers to demand, respectively, urine samples from persons merely *suspected* of being reckless drivers, and blood samples from *suspected* virus carriers. Two other bills, Bill C-262 (MP Peter MacKay) and Bill C-264 (MP Keith Martin), are very similar.

Two other bills tabled this year deal with an issue discussed in this report and the 1998-99 annual report (pages 26-27): census records. Both Senator Lorna Milne and MP Mac Harb tabled bills (S-15 and C-312 respectively) that

would have Statistics Canada transfer to the National Archives all census records beginning with the 1906 returns. The National Archives of Canada would then make the records publicly available 92 years after the census. As well, MP Jason Kenney moved Motion M-160, calling for the release of the 1911 census records as soon as they are transferred to the National Archives in 2003. The Privacy Commissioner continues to oppose the disclosure of identifiable census information collected under the legal obligations of confidentiality of the *Statistics Act*.

One last bill that could have negative privacy impact is MP John Bryden's Bill C-264. This bill would amend the *Access to Information Act* to require federal institutions to disclose information older than 30 years (including personal information), and personal information that can legally be released to third parties (even if a federal institution considers it should be protected). The first obligation would completely disregard the protections of the *Privacy Act*, which requires individuals' consent for disclosure of their information unless a law authorizes otherwise, or they have been dead for more than 20 years. The second obligation removes the critical discretion the *Privacy Act* gives heads of federal institutions to determine whether they should disclose individuals' personal information to third parties. The Privacy Commissioner, while supportive of Mr. Bryden's ultimate goal of a more transparent and accountable federal government, believes that Bill C-264 should be amended to specifically exclude personal information from its scope.

A checklist for privacy implications

The Office considers several elements when reviewing a bill or proposed regulations for possible privacy implications; among them, does the proposed bill

- specifically mention the *Privacy Act* or Bill C-6?
- create or abolish an agency subject to the *Privacy Act*?
- create, change or stop a collection of personal information (e.g., the gun registry)?
- provide for powers of entry, search and/or seizure (e.g., taking DNA samples)?
- provide for, or result in monitoring or surveillance of individuals?
- create, change or stop data matching or sharing activities?
- propose a new use for information already collected?
- grant an organization the right to access someone's personal information?

- expand, limit or prohibit disclosure of someone's personal information?
- require publication of, or make publicly available, personal information?
- impose fees for, or restrict someone's access to, his or her own personal information?
- require personal information to be kept for a stated period of time?
- require personal information to be destroyed?
- make improper collection, use or disclosure of personal information an offence?
- propose a new technology that is known to invade or is suspected of invading personal privacy?

Cleaning up money laundering: Update on the Proceeds of Crime Act

In last year's annual report, we discussed the government's plan to strengthen and modernize existing legislation to detect, prosecute and deter illicit money-laundering activities. Those efforts were embodied in the *Proceeds of Crime (Money Laundering) Act*, now before the House as Bill C-22. We had several reservations about uncertainties in key elements of the bill. While the government expects to clarify some in regulation, others remain outstanding.

One abiding concern is whether persons or organizations subject to the legislation (such as banks and investment brokers) must tell their clients, and obtain their consent, before collecting information authorized under the bill, as well as advise them of disclosures to the Financial Transactions and Reports Analysis Centre (the Centre). Or will they routinely collect and disclose clients' information without notice on the grounds that notification could prejudice the use of the information for investigative purposes, even if no formal police investigation has been launched? Notification of purpose is a key data protection principle, and it is unclear whether Bill C-22 will adequately honour the principle.

The need to collect such details as the amount of the suspicious transaction and the denomination of the bills will be self-evident to the parties, but not the additional information government could require to determine that the transaction is suspicious. For example, the government still needs to clarify what information it may need about the circumstances of the transaction, and about recipient's duty to confirm the accuracy of the individual's claims about the transaction. The government's intention is to address these

concerns in the form of guidelines that will be developed on an ad hoc basis by the Centre and commercial enterprises subject to the new reporting requirement.

In last year's annual report we cautioned against persons subject to the draft legislation being called upon to make overly subjective and speculative assessments of a client's character and circumstances. We also cautioned against such persons being called upon to make additional inquiries about the client or the transaction itself in order to validate whether first impressions are well founded, lest citizens be forced to perform a role akin to that of state investigators. For these reasons, we favour an approach that would rely on simple and objective criteria based on the transaction that would be prescribed in regulation, rather than through guidelines.

The bill is unclear on several questions. One of these is the transaction details that would trigger the duty to report it to the Centre. A simple monetary threshold would not necessarily be one of the "prescribed conditions" that engage the reporting duty; in fact a monetary threshold may not apply at all in certain transactions. For example, would a client paying more than the posted exchange rate or transaction fees to facilitate a money order transaction be sufficient to trigger the reporting scheme, regardless of the amount?

The draft regulations have established two benchmarks on the amount of money that will trigger reporting: two or more transactions on the same day totalling $10,000 or more in cash, and any transaction involving five or more $1,000 bills. The latter is a dramatic reduction in the financial reporting threshold. Although this low financial threshold might increase the likelihood of capturing petty criminals, it will also likely capture many innocent transactions. (Independent of this legislation, the government has already taken steps to control money laundering by announcing that the Bank of Canada will no longer issue $1,000 bills.)

"THIS FORM PLEDGES THAT WE'LL NEVER DIVULGE YOUR PERSONAL DATA UNLESS WE HAVE A SOUND FINANCIAL REASON FOR DOING SO."

The simple reporting to the Centre of a transaction deemed suspect, of course, does not in and of itself trigger a

formal investigation. To assess whether there are reasonable grounds to suspect that the monies involved constitute "proceeds of crime," the Centre must analyze this information in relation to information gleaned from other sources, including information volunteered to the Centre pertaining to the individual under suspicion, information obtained from law enforcement bodies and information obtained from other government bodies or agencies deemed relevant to money laundering.

If information "relevant to money laundering" may be construed as any information which may be useful in assessing whether a given individual was engaged in some irregular or illicit activity, then the range of information available to the Centre would be very broad indeed. The Centre could, in addition to information pertaining to an individual's criminal history, amass information relating to an individual's employment, financial transaction and travel history, as well as information relating to an individual's income status, business or professional relations, and possibly even personal relations.

In our view, the categories of information, as well as the sources from which the information is derived, should be more clearly defined in the legislation itself, or in regulation. This would limit that information that may be collected by the Centre to only those data elements directly related to and demonstrably necessary for the proper exercise of the Centre's mandate.

Once the Centre has determined that a given transaction likely involves the proceeds of crime, the Centre is authorized to disclose certain "designated information" to specified bodies including the police or RCMP, the Canada Customs and Revenue Agency, the Canadian Security Intelligence Service and the Department of Citizenship and Immigration. At present, "designated information" consists of key identifying information, such as name, date, place where the transaction occurred, the account number, and the value of the transaction.

The danger is that these data elements may be expanded to include other information relating to the transaction. The Office of the Privacy Commissioner maintains that information constituting "designated information" must be kept to a bare minimum. Otherwise, the Centre could become a mere conduit through which forensic evidence is channelled to law enforcement bodies, thereby circumventing the rigorous standards and procedures normally applied to the collection of evidence in respect of criminal investigations.

Although the Centre is expressly subject to the federal *Privacy Act*, a great unresolved question is precisely what rights an individual may effectively

exercise with respect to personal information held by the Centre. For example, will the new legislation honour an individual's rights under the *Privacy Act* to access and request correction of information held by a federal government institution? Or will such rights be denied on a routine basis because the information was obtained in the course of a lawful investigation? We can only hope that the *Privacy Act* will prevail.

Clearing customs: Flying the unfriendly skies

Last year's annual report described U.S. customs officials' ability to collect information from airlines about people travelling through Canada en route to the United States. U.S. Customs officers at major Canadian airports could collect details such as where the passengers made their reservations, how they paid, what special meals they ordered and what seats they chose, then use the profiles to deny them entry into the United States. Canadian customs officials are not allowed to use profiling to make decisions about travellers, yet the *Preclearance Act* was effectively permitting the practice by foreign officials on Canadian soil. We worried that Canada Customs would adopt similar measures.

The concern was well founded. This year we discovered that Citizenship and Immigration Canada (CIC) is cooperating with the Canada Customs and Revenue Agency (CCRA) on a passenger profiling system to expedite customs clearance.

The proposed scheme involves commercial airlines collecting travellers' personal and travel information and transferring it to Canadian customs and immigration officials at the destination before the passengers' arrival. From the information, the agencies would create profiles to select "high-risk" travellers for primary or secondary questioning. The original proposal acknowledged that both the *Customs Act* and the *Immigration Act* would have to be amended to implement the system.

> ***To live by the worst-case scenario is to grant the terrorists their victory, without a shot having been fired. It is also alarming to think that the real battles of the new century may be fought in secret, between adversaries accountable to few of us, the one claiming to act on our behalf, the other hoping to scare us into submission.***
>
> **--- Salman Rushdie, 2000**

Staff examined the proposal and found it required a wide range of data elements—32 in total—that customs and immigration considered necessary to effectively identify "suspicious travellers". The information was

to include not only name, citizenship, passport number, date of ticket purchase, travel history, and country of departure, but also lifestyle information such as income, class of ticket, number of checked bags, dietary preferences and even whether or not meals were eaten. We questioned how some of this information was relevant to a proper assessment of an individual's right to enter Canada and even the airlines' ability to provide the details.

Extensive consultations with CIC and CCRA led to a significant cull of the most intrusive and irrelevant details; the data elements have been reduced from 32 to 15. We sought clarification of the term "travel history", urging that this information be confined to cancellations and "no-shows".

Given the substantial personal information being gathered, and the dangers inherent in profiling, we urged both organizations to spell out required data in law rather than regulation. We also advised amending the *Immigration Act* and the *Customs Act* to provide clear safeguards against government using the information for secondary or unrelated purposes. Finally, we proposed that since pre-clearance is supposed to be a convenience for travellers, the decision to participate should be theirs. Those choosing not to participate would undergo the normal, and potentially slower, customs and immigration checks. The proposed scheme gives the discretion to participate to the airline, not the passenger.

Providing taxpayer/business information to provincial statistical agencies

In May 1999, the Department of Finance and Revenue Canada (now the Canada Customs and Revenue Agency) informed the Privacy Commissioner of proposed amendments to the *Income Tax Act* and *Excise Tax Act*, that would allow tax filer information to be shared with provincial statistical agencies.

The government initially proposed making an addition to section 241(4) of the *Income Tax Act* (and section 295(5) of the *Excise Tax Act*), that would read

> An official may provide taxpayer information to an official, solely for the purpose of enabling a statistical agency of a province to obtain statistical data for research and analysis and, notwithstanding paragraph 17(2)(a) of the *Statistics Act*, in the case of taxpayer information provided by the Chief Statistician, irrespective of when the information was collected.

We were concerned at the amendment's potential scope for disclosing individual tax filer's information. Our further inquiries revealed

- The amendment is intended to permit Statistics Canada to provide provincial statistical agencies financial information on incorporated and unincorporated businesses that it obtains from the Canada Customs and Revenue Agency.
- Statistics Canada has always been a key source of Canadian business data for provincial statistical agencies. Statistics Canada relies on sharing agreements to provide provinces the information they need to research and analyze social and economic activities.
- Provinces have a growing need for detailed financial information from small and medium businesses to improve their economic statistics. Statistics Canada is gradually making more extensive use of income tax records instead of surveying businesses directly, thus reducing the response burden.
- Statistics Canada would share the data with provincial agencies that are governed by provincial statistics acts and so subject to strict terms and conditions on their use of the data.
- Government has no intention whatsoever of sharing tax information about individuals unless they have submitted information about operating a business in their income tax return.
- Provinces would have access to the business tax data through a Discretionary Disclosure Order signed by the Chief Statistician under section 17(2)(a) of the *Statistics Act*. Statistics Canada's Policy on Discretionary Disclosure requires that the party obtaining any such information provide an undertaking of confidentiality and agree to use the information solely for statistical and research purposes. The undertaking would prevent any further release of data without the express authorization of the Chief Statistician, and any subsequent release would also be constrained by the provisions of the *Income Tax Act*.

The Privacy Commissioner made four recommendations to the Department of Finance, Statistics Canada and the Canada Customs and Revenue Agency:

- Contrary to the proposed wording, the amendment should clearly state that the information to be disclosed concerns businesses or individuals who have submitted information in their income tax return about the operation of a business;

- Ideally, Statistics Canada should provide the information only after the amendment comes into force—there should be no retroactive effect, or at the very least the amendment should specify a year;
- Tax filers, especially small and medium businesses, should be told through brochures or pamphlets who has access to their income tax information and for what purpose; and
- Arrangements between Statistics Canada and each provincial statistical agency should clearly state that the statistical information would be used solely for research and analysis purposes, regardless of whether provincial legislation permits other administrative uses.

After much discussion, all parties accepted the recommendations. Statistics Canada and Canada Customs and Revenue Agency officials are currently devising the best and most cost-efficient means of informing Canadians of this intended further use of their business tax data. Notification will happen once the legislative amendment has received Royal Assent. Although the government has recently decided not to amend the *Excise Tax Act*, it has changed the wording of the amendment to section 241(4) of the *Income Tax Act*. It will closely resemble the following

> An official may provide taxpayer information in respect of the 1997 or following taxation years to an official solely for the purpose of enabling the Chief Statistician to provide to a statistical agency of a province statistical data to be used for research and analysis, if the information relates to:
>
> (i) a corporation, or
>
> (ii) the computation of the income from business of an individual who, according to a return of income filed by the individual or a notice of assessment or reassessment in respect of the individual, carried on a business at any time in the 1997 or following taxation years, and notwithstanding paragraph 17(2)(a) of the *Statistics Act*, despite when the information was collected.

These amendments are an excellent example of how government can improve privacy and administration by consulting the Privacy Commissioner's Office when considering new data sharing arrangements affecting Canadians. The proposed amendment to the *Income Tax Act* is now more specific and prevents any misinterpretation of its intended scope and purpose. The proposed amendment will be included in this fall's Budget Bill.

Filling the gaps: A charter of privacy rights

One of the Privacy Commissioner's goals over the last decade has been to fill some of the gaps in Canada's patchwork of privacy protection. Passage of Bill C-6 has filled one major hole; the *Personal Information Protection and Electronics Documents Act* gives Canadians important new rights concerning the private sector's collection, use and disclosure of their personal information.

While passage of C-6 is a major milestone in the evolution of privacy protection, the battle is not yet over; Canadians still do not have a constitutionally protected right to privacy. We hope that this will change with Senator Sheila Finestone's proposed Charter of Privacy Rights.

> *Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.*
>
> — Justice La Forest, 1988
> (R. v.Dyment)

Senator Finestone's proposed charter would give every individual a right to privacy. Any interference with an individual's privacy would be considered to infringe on that right unless it is reasonably justified and the individual's consent has been obtained (except when it is impossible or inappropriate to do so). The onus lies with the organization or individual proposing the measure to demonstrate that the interference is reasonably justified—the charter includes a reasonable justification test. The charter requires the Minister of Justice to review all government bills and regulations to ensure that they comply with the charter. Any inconsistencies are to be reported to Parliament and the Privacy Commissioner—a measure the Privacy Commissioner has long advocated.

According to Senator Finestone, the charter would serve "as an overarching privacy rights framework for Canada". We take this to mean that the charter would act as a set of "first principles" that would support both the federal *Privacy Act* and the new private sector legislation. At present, for example, a government institution can effectively override the protection in the *Privacy Act* if legislation is passed specifically authorizing it to disclose personal information, thus complying with section 8(2)(b) of the act. The proposed charter would require the institution to demonstrate the justification for the privacy infringement. As well, the charter would provide a possible remedy

for someone whose privacy is threatened by the legislation, for example, by allowing the individual to challenge the law. This would go some way towards meeting our objective of establishing the primacy of the *Privacy Act* over all other federal legislation dealing with the collection, use and disclosure of personal information.

The charter would also go a long way towards meeting another of our goals, a constitutional right to privacy. In 1991, the Privacy Commissioner appeared before the Special Joint Committee on a renewed Canada to advocate amending the *Canadian Charter of Rights and Freedoms* to give Canadians clear constitutional privacy protection. Given the likely reluctance of any government to reopen the *Charter of Rights and Freedoms* in the near future, the proposed privacy charter is an alternative we can enthusiastically support.

Senator Finestone has been one of privacy's best friends in Ottawa. Among her many accomplishments one stands out, her role as the chair of the House Standing Committee on Human Rights and the Status of Persons with Disabilities. The committee's 1997 Report, *Privacy: Where do we Draw the Line?* makes a thoughtful and compelling case for recognizing privacy's fundamental value to Canadian society by, among other things, introducing a privacy charter. We are happy to see that her commitment to privacy protection has carried over to her new position as a Senator.

Issues Management and Assessment Branch

The Issues Management and Assessment Branch monitors government programs and legislation, researches emerging issues, and provides the Commissioner policy advice and communications support.

A few portfolio leaders provide the Office a contact point with federal agencies to resolve issues before they lead to complaints. As well, portfolio leaders conduct formal audits and follow-ups.

The branch depends on a handful of researchers to keep the Office current on other developments that concern privacy. This includes examining proposed legislation and government programs, researching trends in Canada and abroad, responding to organizations' requests for the Office's review of proposals with privacy implications, and providing background for the Commissioner's public appearances.

The branch's responsibility for both communications and Parliamentary liaison enhances the Commissioner's public communications. Briefing the Commissioner for appearances before Parliamentary Committees, writing speeches and much of the annual report content, and developing material for the Office's web site are among the branch's key functions.

As well, branch staff handle more complicated questions and inquiries that fall outside the Commissioner's mandate. They act as a contact point for international data protection commissioners on privacy protection in Canada and support the Investigations Branch, providing background and obtaining any needed expert advice.

Assessing Privacy Impacts

Canadian society has undergone many changes over the last few decades: rapid population growth, increased demands on state resources, privatization of governments activities, and exponential development and availability of information and communication technologies.

New programs, products, services and technologies can alter Canadians' privacy or change our privacy expectations. Given their potential effect on Canadian society, it makes good political, business and social sense to evaluate these initiatives before they are implemented. Environmental impact assessments are a regular feature of new proposals and have proven their worth. New technological developments make privacy protection as

important an issue at the beginning of this century as environmental protection was at the end of the last. Privacy impact assessments have come of age.

These assessments serve a number of purposes

1. They act as an early warning and planning tool;
2. They avoid pitfalls in new developments, preventing adverse publicity, loss of credibility and public confidence—not to mention possible legal costs, remedies and sanctions;
3. They forecast and/or confirm the privacy impact of proposals on individuals and groups;
4. They assess a proposal's compliance with privacy protection legislation and principles;
5. They determine the corrective actions and strategies required to avoid or overcome the negative impact; and
6. They increase Canadians' privacy awareness, informing them of the details of the proposal and involving them in its design, acceptance and implementation.

The assessment process

Who: The best party to conduct an assessment should be the public or private sector organization making the proposal. While data protection and privacy commissioners have expertise, no one knows the detailed proposal better than those designing the product or service. They are best suited to answer the questions an assessment raises. However, to guarantee the assessment's objectivity, the organization should consult affected Canadians, subject the completed assessment to an independent privacy expert for review, and make the completed assessment available to the public.

When: Logically, an assessment should be part of the proposal's design phase and be undertaken as soon as the organization decides to examine its feasibility. While some assessments may be finished before implementing the proposal, some could continue during implementation. And others may never end, becoming an integral part of ongoing quality control.

What: While each assessment will vary with the circumstances and nature of each proposal, all should be assessed against internationally accepted information privacy principles, applicable privacy protection laws, as well as the privacy expectations of affected Canadians.

How: Each assessment should address and document the following elements

- Proposal: The organization should thoroughly describe the proposal, detailing its components and timetable, providing background information, and outlining the scope of the proposal (who and what it will affect);
- Impacts: The organization should then describe the positive and negative impacts (both known and suspected) of the proposal on Canadians' privacy. The organization should describe the cumulative nature of each impact, as well as its duration, frequency, intensity, probability and scope, then grade each impact (low, moderate or high);
- Necessity: The organization should justify the necessity (other than commercial gain) for the proposal itself, its timing, and its negative impact;
- Compliance: The organization should assess its proposal against internationally accepted privacy principles, applicable privacy protection laws, and the privacy expectations of affected Canadians; and
- Alternatives and solutions: The organization should identify both alternatives that would avoid the impacts and compliance issues identified above, and solutions that would eliminate or mitigate a given impact or compliance issue.

The Office conducts assessments of some government or private sector proposals, some on its own initiative (to better understand the details and impact of a given project or technology), and others at the specific request of the organization. For more information on privacy impact assessments, a list of information privacy principles or of applicable privacy legislation, please contact us or visit our Web site.

Data sharing at the Canada Customs and Revenue Agency

Early in 1995, the Office surveyed all the federal institutions that were subject to the *Privacy Act* to determine how much formal and informal sharing and data matching of personal information was taking place. Of the institutions that reported sharing personal data, Revenue Canada (now the Canada Customs and Revenue Agency) indicated that it was sharing a variety of client information with other federal, provincial and foreign government institutions to help them administer their programs more effectively and economically. The main rationale for data sharing is it avoids collecting data that has already been collected by another institution or government from

the same persons, businesses or organizations. The information shared ranged from computer tapes of the entire tax filing population to small quantities of information in paper format.

With its survey response, Revenue Canada attached a list of the more than 200 written agreements that it had with other government institutions, along with a general description of the purpose and the legal authority for the data sharing. The department reported that all of these exchanges of information were being done in accordance with the legislation it administers (i.e., the *Income Tax Act*, the *Excise Tax Act*, the *Customs Act*, etc.) and with the provisions of the *Privacy Act*, and were referenced in the *Info Source* publication.

The number of sharing agreements at Revenue Canada has increased significantly since 1995. According to the Revenue Agency, it now has more than 300 written agreements for the exchange of information with outside organizations. Apparently, this number is growing rapidly due to increased pressure to deliver services more efficiently and effectively as well as the Agency's emerging role administering benefits for outside partners.

Given the large number of these agreements, the breadth of their purposes and the partners that are involved, the Office advised the Revenue Agency last December of its intent to conduct an informal review of its sharing agreements. The purpose of our review will be to determine the degree to which these exchanges of information are in compliance with the provisions of the *Privacy Act*. Particular attention will be given to those sharing agreements that started before the *Privacy Act* was put in place. The review will also determine whether any of these sharing agreements are technically speaking data matching activities as defined in the *Treasury Board Policy on Data Matching* about which the Privacy Commissioner should have been notified.

The Canada Customs and Revenue Agency has assured the Office of its entire cooperation during the review.

Conducting client survey research

Last year, the Office received several inquiries from federal institutions considering using private polling firms to conduct client satisfaction surveys. All wanted to know whether disclosing clients' personal information to the polling firm to conduct the survey would violate the *Privacy Act*.

In each case, we were satisfied that the department's sole purpose for conducting the survey was to assess its clients' satisfaction with the services and determine how to improve its service. We recognize that it is reasonable for public bodies to have some contact with their clients to improve client service but no matter how valid the need, three important requirements must be met before an institution discloses its clients' personal information to an outside survey firm. These are

Authority to collect: The institution must first ensure that it is legally authorized to collect the information the survey will gather. This means that the survey must relate directly to the institution's operating programs or activities.

Authority to disclose: A government institution's authority to collect client information does not necessarily mean that it is authorized to disclose the information to an outside organization to conduct a survey. Some statutes expressly define and limit the circumstances in which personal information may be disclosed; the institution should ensure there is nothing in its enabling legislation that could prevent any such disclosure to a private survey firm.

Compliance with the Privacy Act: Assuming the institution's own legislation does not prohibit disclosure, the institution must then ensure that disclosure conforms with the *Privacy Act*. Under the act, clients' personal information cannot be disclosed to an outside organization for a survey unless: (a) the clients were told when the information was collected that it could be used or disclosed for surveys; (b) the clients have consented to that use or disclosure or (c) the disclosure is permitted by one of the disclosure provisions in section 8(2).

In certain circumstances, departments could justify disclosures to a survey firm as a "consistent use" of the information (section 8(2)(a)) but only if using client information for any survey is sufficiently related to the program to qualify as a "consistent use" under section 7(a).

The act does not define a "consistent use" for the purpose of these sections. However, Treasury Board guidelines on administering the *Privacy Act* state that "a consistent use must have a reasonable and direct connection to the original purpose for which the information was originally obtained or compiled." The guidelines go on to say that the connection must be "so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out." The test has both an objective element—the reasonable and direct connection

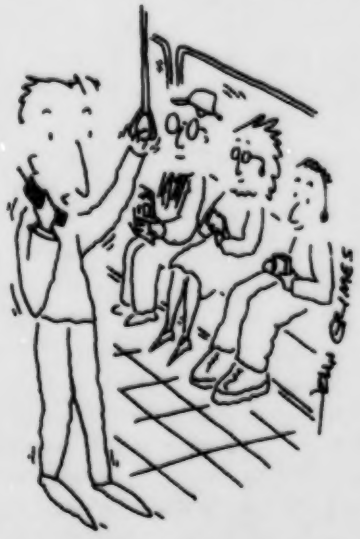
with the original purpose for which the information was collected—and a subjective element—a reasonable individual would foresee the institution using the information in that way.

Given the difficulty of assessing clients' reasonable expectations, departments should employ the "consistent use" provision for disclosing information to survey firms only under exceptional circumstances. This is, however, the least desirable method of disclosing information about clients or customers whose cooperation the government is seeking. It is invisible at the outset and often prompts angry reaction when the survey company calls. A more privacy-sensitive approach would be to obtain the clients' consent.

We encourage institutions to make every reasonable effort to advise clients at the earliest opportunity that a survey firm could contact them in the future. Departments should also describe for clients the statutory authority for the survey, the purpose, how the results will be used and why they have been selected. Clients should also be told that their participation is voluntary, they may refuse to have their personal information disclosed, and they may "opt-out" of any future client surveys.

If the survey is to be conducted regularly, then the institution must tell clients when it first collects the information, and seek their consent (by opting in rather than opting out). The institution must also report the survey in the appropriate Personal Information Bank description in *Info Source*.

Although using an outside agency to conduct a survey does not itself contravene the *Privacy Act*, the institution is responsible for taking all necessary measures to minimize any loss of privacy such a decision would entail. For example, the institution should disclose only those client details the survey firm must have to construct a sample of respondents and to contact the selected individuals. Whenever possible, the institution should minimize the intrusion on its clients by drawing the survey sample itself, thus eliminating disclosures of those not selected.



"DON'T BREATHE A WORD OF THIS TO ANYONE."

Should this option not be practical or feasible, the institution could consider providing the survey firm with a master list of clients (with personal identifiers masked) from which the firm can choose the required number of respondents. Only when the firm has chosen the required number, would the institution disclose the matching personal identifiers.

Government institutions are responsible for ensuring that their clients' personal information is protected during the survey. They should specify in the contract that all the personal information the survey firm is provided or collects during the contract is deemed to be under the institution's control and consequently is subject to the *Privacy Act*. The contract should also contain explicit clauses concerning the use, collection, disclosure, security, retention and disposal of the personal information the firm obtains as a result of the contract. Among other things, the contract should also require that

- The contractor inform respondents (prior to collection) that the information is being collected on behalf of the contracting institution; the purpose of the collection and how the results will be used; that individual replies will not be made available to the contracting institution in an identifiable form without the respondent's informed consent; that response is voluntary and refusal to reply will in no way affect their entitlement to services and/or benefits;
- The contractor will destroy the key permitting it to link the statistical data to individual respondents once the data has been compiled; and
- Once the survey is completed, the contractor will, in accordance with the *Privacy Act*, dispose of all information provided by the contracting institution, and return to the contracting institution all information collected during the survey in a non-identifiable format, unless specified by the respondents.

Before deciding whether to survey their clients, federal institutions must determine the impact such a survey could have on individuals' privacy. A survey may not necessarily be the best instrument for measuring service quality or planning policies and programs. Institutions should first consider alternate sources of information, eliminating any need to disclose personal information to a third party.

Review of Firearms Registry/Canadian Firearms Centre

Previous annual reports have raised the privacy issues inherent in the government's creation of the national Firearms Registry and Office staff have spent considerable time examining the program and its privacy implications.

Despite some progress, problems remain among different jurisdictions concerning individuals' rights (and means) of access to personal information in the registry. In addition, the many partners involved, operational inconsistencies from one province to another, and the complex physical and technological interconnectivity of this program have raised questions about the amount of highly detailed sensitive personal information Firearms Officers need to meet their obligations under the *Firearms Act*.

In January 2000, the Privacy Commissioner began a review of the Firearms Registry to thoroughly assess its personal information handling practices. This review includes on-site visits to the Central Processing Site in Miramichi, NB, to the federally-and provincially-administered Chief Firearms Offices in some provinces, as well as the Canadian Firearms Centre and Registry in the National Capital Region. At a minimum, the Privacy Commissioner expects this review to deal with all the questions and complaints he has received to date. The Deputy Minister of Justice has welcomed the review and awaits any observations and recommendations that would help the Canadian Firearms Centre meet its requirements under the *Privacy Act*.

Data matching proposals—births and deaths with Canada Child Tax Benefit database

The proposed matches:
In August 1998, the Canada Customs and Revenue Agency (CCRA) told the Privacy Commissioner it intended to match the list of families receiving the Canada Child Tax Benefit (CCTB) with all deaths registered by provincial vital statistics agencies. Then, in October 1998, the Commissioner was alerted to a second match of the same list, this time with all new registered births. The matches were intended to identify families who are claiming CCTB but should not, and those who are not but should.

These two proposals were prompted by the Auditor General's 1996 report, which found that the CCTB program lacks fundamental checks and balances. The Auditor General observed that CCRA should find better ways to serve low income families using innovative technology, and by forging partnerships with provinces.

Background:
The CCTB is a tax-free monthly payment to help eligible families meet the cost of raising children under the age of 18. Included with the CCTB payment is the National Child Benefit Supplement, a joint federal-provincial-

territorial benefit for low-income families. CCRA uses the information collected on CCTB application forms to administer both these programs, as well as several provincial and territorial child benefit and tax credit programs.

CCRA automatically recalculates benefits each July for the period from July to June, once it receives parents' income tax returns showing total net income. Parents must provide proof of birth if the child was born outside of Canada, or if the child was born in Canada and is at least one year old. To recalculate eligibility, CCRA needs to be advised of any changes of custody (including death of child), marital status, tax reassessments, citizenship/immigration status, and address (unless benefits are deposited directly).

While the Privacy Commissioner does not argue that collecting provincial vital statistics may help CCRA administer the tax benefit program, several issues need to be addressed before the Commissioner can endorse the sharing. The problem with data matching very simply is that it involves using an individual's personal information without knowledge or consent for purposes for which it was not collected. This violates the spirit of the *Privacy Act*'s fair information code. The sharing of information between provincial vital statistical agencies and CCRA also raises concerns about the confidentiality and security of the information.

Although matching death registry information reveals an apparent revenue loss because as many as 25 per cent of parents do not advise CCRA of a death, this data match raises significant privacy concerns and it may also result in serious allegations that parents are fraudulently benefiting from the death of a child. With respect to the use of birth information, the Privacy Commissioner is not convinced that the five per cent of parents who do not apply for the benefit deserve such an intrusive invasion of privacy, particularly when the institution already has an extensive public awareness process in place.

Early in December 1999, the Office sent its preliminary review of the proposals to CCRA; we await the Agency's response.

Incident investigation—loss of laptop in Halifax —Correctional Service Canada

In January 1999 someone broke into Correctional Service Canada's Halifax Area Parole Office and stole a laptop computer, jacket and set of keys belonging to a contract employee. CSC convened a Board of Investigation to

inquire into the theft because the laptop contained psychological information about 130 offenders (all of whom were advised). The Board's report found the following

- The data on the laptop consisted of 130 offenders' self-administered psychological test results, as well as individual summaries including their names, ages, Federal Penitentiary Service numbers, most recent convictions, list of tests completed, and interpretation of the test results.
- The offenders had used the laptop extensively and knew its location.
- The office has access to a fire exit door leading to a common area, an elevator and stairwell, and anyone could have noted that the unlocked door provided a quick exit from the office.
- Any offender or employee could access the contents of the laptop, which had a modem for communicating with the Internet.
- The laptop containing sensitive personal information was routinely left unattended. At times offenders were also left unattended.
- CSC had not updated the security office procedures and policies for some time. Employees were unclear about the security requirements, and there were serious deficiencies in overall physical and information technology security.

The Board of Investigation report led to a thorough review of security procedures. CSC has taken several other measures, including

- Making security policies a standing agenda item at district meetings;
- Including a security awareness component in its in-service skills training sessions;
- Using only one laptop (which belongs to CSC, not a contractor) for offender self-administered psychological tests. Staff will use a different computer to prepare summary reports;
- Transferring the information to diskette to prepare a report, and clearing the laptop's hard drive each time an offender completes the test;
- Accompanying offenders at all times, even during the tests. All visitors and offenders must check in with reception on arrival and cannot enter the work area directly;
- Removing the modem from the laptop, thus preventing offenders from having access to the Offender Management System, CSC e-mail or the Internet; and

- Installing a lock on the fire exit door to prevent entry from the outside.

Unfortunately, the laptop was never recovered and there is no way of knowing what use (if any) the thief made of the information, or whether the thief had any interest in the contents. We can only hope that, if the laptop was sold, its contents were purged. Obviously the Halifax Area Parole Office's handling and protection of sensitive personal information was seriously deficient but the Commissioner was satisfied with CSC's corrective measures.

Public interest disclosure—medical information about a deceased member of the Canadian Armed Forces

In order to help the widow of a former Armed Forces member settle a life insurance claim, National Defence proposed releasing a copy of the last two years of the member's medical records to the insurance company.

The Privacy Commissioner's staff questioned the need to release the medical file; most pages had no relevance to the specific medical condition of interest. Also, given that the medical records had to be severed from other sensitive information, the insurance company was unlikely to be satisfied with the severed package and question what had been removed from the file. There was a risk the claim would remain unsubstantiated.

Following discussions with the Privacy Commissioner's staff, National Defence agreed to provide the insurance company with only the relevant information. National Defence's Director of Medical Policy wrote to the insurance company confirming that the member had not suffered from the specific medical condition of interest to the claim.

The Privacy Commissioner was satisfied. Although the letter to the insurance company disclosed personal information, the invasion of privacy was greatly diminished. National Defence released no specific records from the military medical file yet it was able to meet the insurance company's requirements. The public interest disclosure was made on compassionate grounds.

Reporting on the administration of the Privacy Act—minimal compliance is not enough

An issue of increasing concern to the Privacy Commissioner is the way in which government institutions report on the administration of the *Privacy Act*. These reports are submitted annually to Parliament, as required by section 72

of the act, with copies submitted to the Commissioner. The Commissioner has dutifully read them, year after year, but with a growing sensation that something fundamental is being missed. This is not a problem of formal compliance with the *Privacy Act*. The reports meet the requirements of the statute. But those requirements are minimal. Given the importance of privacy issues, and the audience for the reports—Parliament—the Commissioner has for some time suspected that government institutions covered by the *Privacy Act* can and should do better.

With some notable exceptions, the reports do not give the reader a broad look at privacy in the institution. A typical report is made up of a statistical report and a narrative statement. The statistical report is a one-page table, setting out things like the number of requests, the disposition of requests, the number of complaints to the Commissioner, the results of complaints, and the costs incurred. The narrative usually begins with a description of the institution and what it does, and how it organizes functions under the *Privacy Act*—who is responsible for what, who reports to whom. Typically, neither of these changes much from year to year. And the rest of the narrative is rarely much more than (sometimes nothing more than) the statistical report restated in full sentences.

The audience for these reports is Parliament. Parliamentarians, particularly when they are looking at programs and estimates, do not need to know about, or only about, the minutiae of administration of the act. They need to know about broad issues with privacy implications. They need to be told about departments' data sharing agreements, and about the impacts on privacy of legislation sponsored by the departments. They need information about the privacy implications of new technology, and of new policies and practices, in a rapidly changing federal workforce and service environment.

In order to report on these things, government institutions need to address their minds to them. Reporting to Parliament—real reporting, not just formal—would encourage them to do so. If institutions know that they have to report seriously on privacy issues, they may begin doing what we have long urged: privacy impact assessments of their program and policy initiatives. In looking at these broader issues, they are welcome to consult with our Office, as did, for example, the Chief Electoral Officer on the issue of the permanent voters' register, or Human Resources Development Canada on the question of a common client identifier.

That we have concerns about the current state of these annual reports should not be taken as criticism of the people who labour to produce them. The professionals responsible for the administration of the *Privacy Act* in

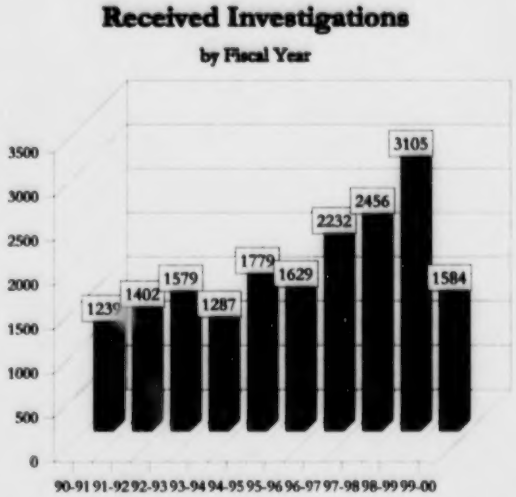
government institutions are the backbone of the act and its protections in everyday life. Better, more substantial reports, covering real privacy issues and commanding the attention of Members of Parliament, would only give them the organizational visibility and importance that they deserve.

The Commissioner encourages the Treasury Board, as the agency responsible for the administration of the *Privacy Act*, to look at ways that this annual reporting requirement can be made more useful and meaningful.

Complaints

After the remarkable surges of the three preceding years, this year's number of incoming complaints dropped to a level not seen since mid-decade. The Office received 1584 complaints in 1999/2000, down significantly from the all-time high of 3105 in 1998/99.

One big reason for the drop was the drastic decline in complaints regarding the government's matching of travellers' customs declarations with employment insurance claims, pending court decisions on the matter. This year, the Office received only 27 such complaints, compared with 1327 in 1998/99 and 963 in 1997/98.



Another significant factor in last year's soaring total was the receipt of 225 time-limit complaints from Correctional Services Canada staff during a contract dispute in 1998. Similarly, in 1996/97, three persons lodged more than half of the 1065 time-limit complaints received. This year, the Office received no such unusual number of complaints from within a single organization or from only a few individuals.

Unlike the numbers for the two preceding fiscal years, the total complaints received in 1999/2000, as well their breakdown by type, conformed to trends previously projected on the basis of initiatives undertaken by the Office of the Privacy Commissioner and federal departments. Specifically, this Office's efforts to deal with those departments most frequently named in time-limit complaints appear finally to have borne fruit. This year's total of time-limit complaints received is down by almost half.

Privacy staff completed 1399 complaint investigations, of which 582 were well-founded, 347 were not well-founded, 82 were well-founded/resolved, 34 were resolved, and 282 were settled during the course of the investigation. The remaining 72 were discontinued for various reasons. (These terms are explained below.)

Completed Investigations by Grounds and Results

for the year ended March 31, 2000

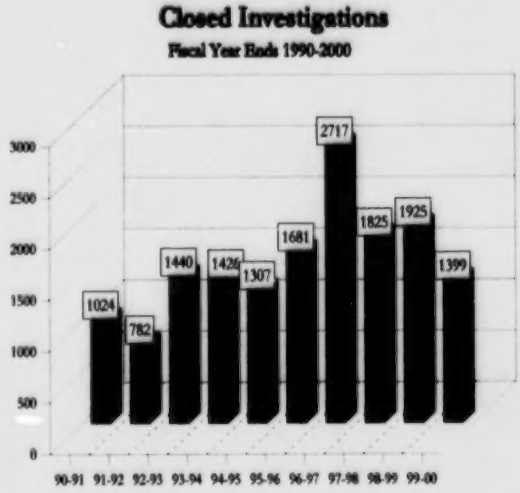
	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Access	**15**	**68**	**172**	**33**	**31**	**184**	**503**
Access	14	67	170	32	29	177	489
Correction/Notation	1	1	2	1	2	6	13
Language	0	0	0	0	0	1	1
Privacy	**73**	**13**	**113**	**28**	**3**	**81**	**311**
Collection	0	2	34	7	1	19	63
Retention & Disposal	5	0	4	2	0	7	18
Use & Disclosure	68	11	75	19	2	55	230
Time Limits	**494**	**1**	**61**	**11**	**0**	**17**	**584**
Correction/Time	25	0	3	0	0	0	28
Time Limits	466	1	33	11	0	11	522
Extension Notice	3	0	25	0	0	6	34
Other	**0**	**0**	**1**	**0**	**0**	**0**	**1**
Other	0	0	1	0	0	0	1
Total	**582**	**82**	**347**	**72**	**34**	**282**	**1399**

During the Commissioner's term

Commissioner Phillips saw the annual number of complaints received increase from 1239 in 1990/91 to a high of 3105 in 1998/99. Excluding this year's unusually low total, received complaints increased by an average of more 10 per cent annually over the Commissioner's term of office, for a grand total of 15,526 complaints.

The table opposite shows total complaints received and investigated in each of the Commissioner's 10 years in office.

Over the years, the Commissioner has also seen a significant change in the types of complaints received. On average, time-limit complaints have decreased, and privacy-related complaints have increased, as proportions of the total. The significance of this trend derives from a difference in complexity.



Time-limit complaints are usually the quickest and easiest to investigate, since for the most part they require intervention only by telephone or by post. Investigations of privacy complaints, on the other hand, tend to be much more difficult and time-consuming, requiring on-site visits (often to distant regional offices), numerous interviews with departmental staff, thorough examinations of files, and detailed reporting of findings. The relative increase in privacy complaints has therefore tended to increase overall case time and workload for investigative staff.

The Commissioner has also noticed a big change in the nature of access complaints over time. Investigations of such complaints used to consist mainly of straightforward reviews of exempted materials. Nowadays, however, many access cases involve efforts to account for documents that are missing altogether. Moreover, shadow files are increasingly involved, and cases are often complicated by the institution's refusal to admit the existence of such files.

As both complainants and departmental Access to Information and Privacy coordinators have generally become more knowledgeable and sophisticated about the application of exemptions, discussions between the parties over the validity of exemptions have become more involved. This has resulted in increases in case time and workload for investigators.

All in all, during his 10 years in office, the Commissioner has observed a trend toward more demanding complaints and more difficult investigations.

Definitions of Complaint Findings and Dispositions

To conclude the investigation of a complaint, the Privacy Commissioner uses one of six terms designating a finding or a disposition:

(1) Not well-founded;

(2) Well-founded;

(3) Well-founded/Resolved;

(4) Resolved;

(5) Settled during the course of the investigation; or

(6) Discontinued.

To assist in distinguishing among the types of findings and dispositions, these terms are defined as follows:

Not Well-Founded

A finding of ***not well-founded*** acknowledges that the investigation uncovered no evidence to lead the Privacy Commissioner to conclude that the government institution violated the *Privacy Act* rights of the complainant. For example, such a finding would be made when

- In the case of a denial of access complaint, all information relevant to the access request had been processed or the exemptions cited by the government institution to refuse access were justified; or
- In the case of a complaint of improper disclosure, the Privacy Commissioner was satisfied based on the evidence gathered during investigation, along with representations by the government institution, that the disclosure of personal information met the requirements of section 8(2) of the *Privacy Act*.

Well-Founded

A finding of ***well-founded*** recognizes that the government institution failed to respect the *Privacy Act* rights of an individual, and that no corrective measures could mitigate the loss of privacy. In other words, while the government institution is at fault, the incident has already occurred and nothing can be done to correct the situation. This category of finding is usually rendered in situations where the institution improperly used or disclosed personal

information or it failed to respond to an access request within the legislated time limits. It could also be used in a situation where the government institution refuses to grant access to personal information, despite the Commissioner's recommendation that it be released. The next step would be to seek a review by the Federal Court of Canada.

Well-Founded/Resolved

A finding of *well-founded/resolved* is rendered in situations where the allegations raised in the complaint were substantiated by the investigation, but the government institution readily agreed to take corrective measures to rectify the problem. Such a finding would be made when, for example a department

- Agrees to release to the complainant information that had been originally exempted; or
- Undertakes to improve a policy or practice to ensure compliance with the *Privacy Act*.

Resolved

The *resolved* category recognizes the need for a finding that is consistent with an ombudsman's role to provide flexibility in complaint resolution. Prior to 1994, the Office struggled with complaints where "well-founded" appeared too harsh to fit what essentially had been miscommunication or misunderstanding.

Examples of *resolved* complaints:

- A misunderstanding or miscommunication has occurred between the complainant and the government institution about what information was sought. Both parties agree to a mutually satisfactory solution.
- The individual has claimed that specific information is missing. The government institution maintains that it has disclosed the records in question, but readily agrees to send the information again.
- The government institution has the right to exempt specific information, but is persuaded by the investigator to exercise the discretion to release it.
- The investigation has identified inconsistent processing of large volumes of information for an applicant, and the government institution is persuaded to release more information to make the disclosure consistent.

In all instances, the Privacy Commissioner's Office assists in negotiating a solution that satisfies all parties. A full and thorough investigation is conducted, and a formal finding is provided to complainants. With a *resolved*

finding, the complainant still maintains the right to pursue the matter in Federal Court.

Settled During the Course of the Investigation
This category is not a formal finding, but rather an acceptable means to dispose of a complaint when the investigation is completed and the complainant is satisfied with the efforts of the Office of the Privacy Commissioner and does not wish to pursue the issue further. For example, the investigator's explanation that the information the complainant believed should have been in the government institution's files cannot be found, either because it was already destroyed in accordance with established retention and disposal standards, or it never existed in the first instance. However, in *Settled* cases, the complainant may subsequently request a formal finding. In such cases, the case is re-opened so that the investigator can submit a formal report, and the Commissioner reports his finding in a letter to the complainant.

Discontinued
This category applies to complaint investigations that are terminated before all the allegations have been fully investigated. A case may be *discontinued* for any number of reasons, for example when the complainant is no longer interested in pursuing the matter, or can no longer be located to provide additional information that is critical to reaching a conclusion. For example, a complainant may move, and not provide this office with a forwarding address or phone number. No formal finding is issued.

Advice for all interviewers: Never assume the person sitting across from you can't read upside-down

A woman informed on her ex-husband in confidence, and the ex-husband found out about it. Had an improper disclosure occurred? For many reasons, this was a tough one to call.

The woman complained to the Privacy Commissioner that Human Resources Development Canada (HRDC) had deliberately and improperly disclosed personal information about her. Specifically, she alleged that an HRDC investigator had revealed to her former husband her identity as a confidential source of information about him. She had previously telephoned HRDC to report her suspicion of a fraudulent employment insurance claim on her ex-husband's part.

It is HRDC policy to protect the identity of informants. In fact, informants need not even identify themselves to HRDC in order to make declarations. This informant, however, had insisted on giving her name and telephone number in case HRDC needed to contact her in future.

Acting on the woman's information, an HRDC investigator called the ex-husband in for an interview, at which he was accompanied by his new wife. The ex-wife's tip proved to be valid, and the upshot of the investigation was that the man's employment insurance benefits were cut off, entirely and retroactively.

Here's where the tale takes a turn. On the basis of his reduced revenues, the ex-husband subsequently filed for a reduction in his child support payments. In the provincial court hearing that followed, the man testified that, during his interview with the HRDC investigator, both he and his new wife had seen a document showing that his ex-wife had made the declaration against him.

After hearing the evidence, the judge granted him a substantial reduction in child support payments. In effect, the ex-wife was thus deprived of a significant amount of much-needed financial assistance for her child. And although the judge made a point of denying that the ex-wife's role as informer had in any way influenced the court's decision, the woman herself remained unconvinced.

Given that the complainant was to some extent dependent on payments from her ex-husband, why had she informed on him in the first place? As often happens in the course of an investigation, many such puzzling questions occurred to our investigating officer about the lives, the relationships, and the motives of the individuals concerned. But, as usual, such questions were beside the point. For a Privacy officer, the only question that really mattered was this: Was it true that personal and confidential information about the complainant had been disclosed to the ex-husband and his new wife during the interview with the HRDC official?

Here are some of the circumstances our officer had to take into consideration:

- From long experience, the HRDC investigator had come to appreciate the value of information sources and the need to protect the identity of informants. In this case, he knew beforehand that the couple to be interviewed would strongly suspect the ex-wife of being the informant (in fact, during the interview they told him so). He knew, too, that the couple would likely be intent on getting from him, in any way possible,

some corroboration of their suspicion. With that in mind, he went to the interview room even more than usually determined not to reveal the informant's identity by any means.

- Even so, for purposes of reference, the HRDC investigator took the case file with him into the interview room, as is customary. The file contained, among other things, the two forms on which the ex-wife's information had been originally been recorded. At the bottom of both forms, the ex-wife's name and telephone number were clearly visible.
- The HRDC investigator believed that he had exercised all due caution in using the case file during the interview. Although the interview room was small and its occupants in relatively close quarters, he had not left the file open or unattended, and he had taken particular care not to allow the couple to see the informant's identity on the forms. He could not deny it categorically, but he strongly doubted whether the couple had been able to catch any glimpse of confidential information.
- Nevertheless, the ex-husband told our investigating officer that both he and his new wife had done that very thing. He said that he had seen his ex-wife's telephone number and what appeared to be her name at the bottom of one of the forms in the investigator's file. His wife, too, he said, had been able to discern some detail on the form—enough that between the two of them they were able to make a positive identification of the ex-wife as the informant.
- Through a *Privacy Act* request, the ex-husband gained access to his HRDC file, which contained the two forms in question. At the bottom of the forms, for purposes of confidentiality, the informant's name and telephone number had been blacked out.

Largely from the convincing manner in which the ex-husband described the blacked-out portions of the forms he had accessed, our investigating officer tended to believe that a disclosure had indeed been made during the interview. But he had to be sure. How likely was it, after all, that the ex-husband could have read one of the forms upside-down? The officer decided to run a test.

Simulating the interview situation, he placed the form on a desk five feet away from himself. Though looking upside-down at the form across a desk at that distance, he found that he was able to read the informant's telephone number quite easily. With only a little more difficulty, he also discerned her name.

This was enough to convince him. He recommended that the Commissioner render a finding of "well-founded" for the ex-wife's complaint. The Commissioner did so, but with one important proviso. The disclosure of confidential information had been improper, but obviously far from deliberate. The Commissioner took pains to point out that HRDC investigator's error had been inadvertent.

A well-founded complaint about a serious matter—disclosure of personal income tax information

In a much-publicized case, the complainant alleged that Revenue Canada had disclosed his personal income tax information to the Manitoba Public Insurance Corporation (MPIC) in contravention of the *Privacy Act*.

In due course, the Privacy Commissioner concluded that the complaint was well-founded. More importantly, he took measures to eliminate what he considered to be a serious privacy violation that had become common practice in Manitoba.

The complainant had been involved in a serious automobile accident. He subsequently filed a claim with the MPIC and, at the same time, signed a consent form. Essentially, the signed form gave permission for the MPIC to conduct its investigation and collect medical and employment records about the applicant.

Among other things, the MPIC needed to confirm the applicant's income. The normal procedure was to have the employer verify the applicant's statement of earnings. In this case, as in many others, a discrepancy arose. Given conflicting information, MPIC officials decided that the only way to get a true picture of the applicant's earnings would be to obtain his tax records from Revenue Canada.

More easily said than done, one might well have thought. After all, a person's tax information is supposed to be confidential. Revenue Canada has a consent form of its own, called a Revenue Canada Authorization. Before any specified tax information may be released to a third party, that form is meant to be filled out with a clear and unambiguous information request and signed by the taxpayer in question. For the MPIC, though, no such trouble was necessary.

An official simply took the MPIC's general consent form, which the applicant had signed, and attached it to a Revenue Canada Authorization,

which the applicant had neither signed nor even seen. Then the official wrote, on the unsigned Revenue Canada form, "See attached authorization". Moreover, the official did not even bother to limit the request to the very specific information the MPIC needed for its investigation. On the face of it at least, the authorization permitted Revenue Canada to disclose not just the applicant's current income, but any and all of his personal tax information over the last five years.

And that is just what the MPIC received—five years' worth of the applicant's tax records in detail. Ask and ye shall receive.

As our investigation revealed, that is what the MPIC *always* asked and received from Revenue Canada. Several MPIC requests for tax information came every week to the local Revenue Canada office. Revenue Canada staff always processed the requests as a matter of routine, never once questioning whether the MPIC's general consent form was sufficient authorization for the release of tax information. And more often than not they were extremely generous in their responses, giving the MPIC far more information than it required for its purposes.

Nor had MPIC officials ever doubted their own authority to access such information. They believed that their general consent form entitled them to the full range of an applicant's tax records, even when they only needed one piece of information.

The Privacy Commissioner could not agree. On the contrary, he could only conclude that Revenue Canada, in releasing the complainant's tax records without his explicit consent, had seriously violated the complainant's rights under the *Privacy Act*. Though regrettably the violation to the complainant could not be undone, the Commissioner took steps to ensure at least that no one's rights would ever be violated in the same way again.

He made sure, first of all, that the complainant's tax records were removed from the MPIC premises. He then underscored, for the benefit of all concerned, the continuing requirement for a clear, unambiguous, and signed consent form for the release of tax information. Finally, he recommended that Revenue Canada terminate the practice of releasing tax information to the MPIC, while the two organizations work out a strict agreement on disclosure of information.

Revenue Canada stopped releasing tax information to the MPIC as of April 27, 1999. The Privacy Commissioner will follow up to ensure that the

eventual information-sharing agreement between the two organisations is appropriate and in full accordance with the *Privacy Act*.

Meanwhile, if the MPIC needs verification of claimants' income, it will be up to the claimants themselves to obtain it from Revenue Canada.

"Smith" the good citizen or "Smythe" the criminal? It's all the same to some computer databases

Three friends went into a store. Two came out with purchases. The third left empty-handed and embarrassed, feeling suspected of being a criminal.

What these friends had set out to buy were firearms, in full compliance with the strict registry procedures currently in place. The three duly filled out the application forms, and the store clerk phoned in for the required computer checks against the database known as FIP—"Firearms of Interest to Police." Two applications went through with no problem, but the third was automatically refused. As a reason why, the computer offered only the phrase "New events against the buyer".

Once refused, the application was referred electronically to Ontario's Chief Firearms Officer (CFO) for his review. Within 48 hours, the CFO overturned the refusal and approved the application.

But questions remained unanswered. Why had it been refused initially? Why had a previous application by the same buyer been approved without a hitch only a month before? What sort of "new events" had the computer check turned up?

The applicant approached the Department of Justice for an explanation. Officials told him that the FIP search had matched his name to an individual having a similar name and date of birth and known to police. For a short while, the applicant was satisfied with this explanation—that is, until the same thing happened to him again.

The second refusal occurred only a month after the first. Once again the firearms application was rejected because of "New events against the buyer." Once again, the applicant was deeply embarrassed to have been thus centred out under the suspicious gaze of store clerks and other customers. And once again, within a day or two, the CFO discovered the mistake, overturned the refusal, and permitted the applicant to make his purchase. The FIP search

had, for the second time, matched his particulars to another person, who was ineligible to buy firearms.

This time, however, the applicant did not accept the department's spoken explanation. One case of mistaken identity, he thought, was understandable, but not two. And he certainly did not relish the prospect of suffering the same humiliation any time he made application for firearms in future, as the officials had warned him was quite likely to keep happening. He decided to delve into the matter by submitting information requests under the *Privacy Act* to both the Department of Justice and the RCMP.

In response to his request for a detailed written explanation, Justice simply sent him copies of the three firearm applications he had submitted. The two applications that had initially been refused yielded no details beyond the original notation, "New events against buyer." The covering response letter said that it was not within the department's mandate to explain, but only to identify and review records requested.

The man subsequently filed complaints under the *Privacy Act*, to the effect that he had not received any written information *explaining* why he had been temporarily denied approvals to purchase firearms.

The FIP system itself was of no use in providing an explanation. Justice officials pointed out to our investigator that FIP transactions are paperless, lacking even the capability to "print-screen" reasons for refusals. But in investigating the corresponding complaint with the RCMP, our officer gained access to other databases that did prove useful.

She was eventually able to identify the person whose name and date of birth had twice been matched to the complainant's. As it turned out, the birth dates were five months apart, and the surnames were about as much alike as "Smith" and "Smythe". That's close enough, apparently, for a phonetically oriented computer.

Our investigator also managed to make some headway in the matter of future applications. In this, she had abundant help from the complainant himself, through numerous telephone calls and letters on his own behalf.

In the end, Justice officials were persuaded to modify FIP so as to dissociate the complainant from the other individual, at least in the present context. They did so by switching off the event code that had been assigned to the latter's latest run-in with police. The department made it clear, however, that if the other person—or, for that matter, *any* other person with similar name,

birth date, or address—ever had further trouble with the law, a new event code would be entered and would probably produce another match with the complainant. If so, he would have to contact the department and have the code switched off yet again.

Even though the name of the other person could not be divulged, and despite the potential inconvenience of further mismatches in future, the complainant was quite satisfied with the progress of the case. It was not inconvenience or delay that he had objected to in the first place. He knew that many other innocent parties—notably, the real Smiths and Tremblays of this country—often had to put up with even greater inconvenience and delay in the process of FIP searches. But neither did the complainant object to the FIP process itself, or even to firearms registry in principle.

All he had ever really wanted was an explanation in writing. He just wanted something he could carry with him, to show friends and clerks and fellow customers that he was not a criminal.

Once assured that our written report to him would include such an explanation, he readily agreed to consider his complaint against the Department of Justice "settled in the course of the investigation."

The Office is currently reviewing the personal information handling practices of the Canadian Firearms Program as discussed above.

Appeal board witness grilled—about irrelevant private matters

After a federal job competition, it is not unusual for an unsuccessful candidate to appeal. It is unusual, however, for an appellant's witness to be humiliated through improper disclosure of personal information. Unusual, but not unheard of, as this case goes to show.

The Privacy Commissioner does not want to hear of it again.

An employee of a government institution lost a job competition within the organization. When she proceeded to file a formal appeal with the Public Service Commission Appeals Board, her union asked one of her co-workers to testify in her behalf. The management side immediately objected to the co-worker's appearing as a witness. In a formal submission to the Appeals Board, institution management explained its objection and concluded with a warning: if this co-worker and a certain other were allowed to testify, the

institution would attempt to discredit not only their testimony, but also their "credibility as witnesses."

Ironically, this co-worker had never even wanted to appear as a witness. In fact, he had initially declined the request. Nor was he known to be particularly sympathetic to the appellant. Nevertheless, the union believed that he had information about the job competition that might support her case, so the Appeals Board issued him a summons, which he duly obeyed.

During the proceedings, institution management followed up on its earlier warning. In cross-examination, the management representative persistently attacked not only the co-worker's testimony, but also his credibility. Soon, however, the questioning began to stray more and more into areas whose relevance the Chairperson of the Appeals Board called into doubt.

At last it strayed into one highly irrelevant and sensitive area—the witness's recent extended sick leave and the medical reasons for it. The questions asked in this regard were pointed, intimate, and informed, betraying much more than a passing acquaintance with the witness's medical history. Indeed, such questions could only have been conceived by someone who had previously accessed and read the witness's personal and confidential attendance records.

The Chairperson soon put an end to the line of questioning, but the damage was already done. Sensitive and confidential information was now out before the Appeals Board, and the witness felt publicly humiliated. A few weeks later, still reeling from the cross-examination, he filed a complaint with the Office of the Privacy Commissioner.

How had the management representative gained access to the witness's attendance records? Quite easily, as our investigation showed. The representative happened to be a personnel manager with the institution. In the normal course of duties, this person had routine access to employees' attendance records, including medical certifications. Management's representative had thereby learned beforehand all about the witness's extended leave, the medical reasons for it, and the subsequent medical treatment. The witness had thus been cross-examined by someone who not only knew his medical history, but also had come to the proceedings with every intention of disclosing it to discredit him.

The management representative knew the history, and as a personal manager was entitled to know. But as a cross-examiner this person was in no way entitled to disclose. Sections 7 and 8 of the *Privacy Act* prohibit federal

institutions from using or disclosing personal information about an individual without the individual's consent except for the purpose for which the information was obtained or for a use consistent with that purpose.

The Privacy Commissioner concluded that the information relating to the witness's sick leave, the nature of his illness, and the subsequent medical treatment had no relevance to the issues before the Appeal Board's hearing. He pronounced the complaint well-founded, and the disclosure a serious matter.

The Commissioner became especially concerned when he learned that this was not the first improper disclosure the personnel manager had ever made. Indeed, from the mounting evidence, it seemed this person was under the misapprehension that the position of personnel manager entitled one to use and disclose employees' personal information however and whenever one pleased.

The Commissioner has advised the institution involved to clarify for that manager and for all its other managers and employees, their obligations regarding disclosure of personal information under the *Privacy Act*. He intends to closely monitor the institution's efforts to that end.

RCMP officer vs. seatbelt violators: Next, he was going to tell their mothers on them

Overall, the RCMP has a remarkably good record at respecting privacy rights. It is perhaps all the more remarkable given the amount and type of personal information the organization collects, and the vast potential for abuse. Yet, as far as the *Privacy Act* is concerned, the Commissioner has usually found the RCMP to be not only among the most law-abiding of federal institutions, but also among the most willing and co-operative in redressing any violations that occur.

But, regrettably, violations do sometimes occur. On occasion, for example, some keen and well-meaning RCMP officer takes an initiative that simply oversteps the bounds.

Last year one such officer, frustrated in trying to enforce the seatbelt law in Alberta, decided that mere enforcement was not enough. He took it upon himself to *reinforce* the law, in his own special way.

An Alberta motorist later complained to the Privacy Commissioner that the

RCMP had improperly disclosed personal information about him. Specifically, he alleged that a copy of a violation ticket he had received for failing to wear a seatbelt had been sent to his insurance company by the issuing officer.

Alas, the allegation proved all too true. Our investigation revealed that the RCMP officer in question had done that very thing—not just once, but several times. The officer himself admitted that over three or four months he had contacted the insurance companies of between 10 and 20 individuals who had previously been ticketed for seatbelt violations.

He explained it as a "pilot project" that he had undertaken on his own initiative. The RCMP was in fact conducting a campaign to increase seatbelt use in the area, but only this one officer had been inspired to take it to such lengths. His reasoning was that, if seatbelt use violators were subjected to increased insurance payments *as well as* fines, they would soon start to buckle up.

It did not seem to have occurred to him that, in taking such action against one kind of violator, he was turning himself into another kind—a violator against Canadian citizens' rights under the *Privacy Act*. Section 8 of the act prohibits disclosure of personal information about an individual without the individual's consent, except under special circumstances as listed in section 8(2) of the act.

The Privacy Commissioner found no such special circumstances applicable in this case. He concluded that the complaint was well-founded, the officer having failed to consider the confidentiality provisions of the *Privacy Act* when the pilot project was initiated. The Commissioner also made a point of informing the RCMP that he considered such inappropriate disclosure a serious breach of individuals' *Privacy Act* rights.

To the RCMP's continuing credit, its officials put an end to the officer's pilot project as soon as they found out about it. At the suggestion of our Office, they also canvassed all Alberta detachments to make sure that no other officer of theirs had been acting upon similar inspiration. The response came back negative. It had been truly a one-man operation.

All in all, then, the officer did not find much favour for his initiative. But what about the insurance companies? With the prospect of charging higher premiums, did they, at least, see some merit in his pilot project?

Some may have, perhaps, but we know for a fact that not all did. It was initially the complainant's own insurance company that brought this matter to the Privacy Commissioner's attention.

The mystery of the missing missive: Canada Post finds after agreeing to seek

This story involves three complaints by one person about two different organizations, and its rather convoluted plot is not entirely resolved even now. But one of our officers was able to get more or less to the bottom of things by persuading Canada Post to look beneath the surface.

Two months after putting in an information request under the *Privacy Act*, the person in question put in his first complaint, to the effect that Revenue Canada was late in responding. While our office was investigating this time-limit complaint, Revenue Canada informed us that it had just responded to the information request by means of a package delivered to the complainant's post office box.

Our office therefore closed the time-limit complaint, designating it well-founded but resolved. The package, however, did not show up.

What soon come to light was that the package had been addressed to the right person but the wrong post office box—wrong by one digit. Revenue Canada and Canada Post began efforts to trace the package. They could find only a receipt indicating that it had indeed been delivered to the correct retail postal outlet, but had been accepted and signed for by a person other than the addressee.

This prompted a second complaint under the *Privacy Act*, to the effect that Canada Post had improperly disclosed the complainant's personal information by permitting another person to accept delivery and sign for the package. Moreover, despite the signed receipt, the package itself was still missing and unaccounted for.

The complainant had himself made inquiries at the retail outlet. Employees had told him that they had searched, but had found nothing. Wherever the package had ended up, they said, it was definitely not there.

Our investigator informed Canada Post that she intended to visit the site anyway. She also managed to persuade the officials to conduct another search of the premises in the meantime and, if the package happened to be

found, to hold onto it until she arrived. Before even setting out, she received a call from Canada Post headquarters, advising her that regional staff had reported the package found at the retail outlet.

When our investigator arrived at the site, Canada Post officials were there to greet her with the good news. The search that she had requested had been successful. The package had been discovered at last, lying on the floor, buried beneath several Christmas parcels and other pieces of mail.

How it had come to be there, the officials could only conjecture. One suggestion was that the carrier under contract to Canada Post may have made the delivery to the retail outlet, but that, when no post office box as numbered on the envelope could be found, the package may simply have been laid aside and forgotten.

But how would that explain the receipt and signature by a person other than the addressee? Canada Post suggested that, on the other hand, the contract carrier may have delivered the package *not* to the retail outlet, but rather by mistake to some third party, who automatically accepted it and signed for it. Then, presumably on emerging from his trance and noticing that the package was not actually addressed to him, that party may have taken it to the retail outlet indicated in the address. There some employee, not knowing what to do with a package for which there was no corresponding box number, may have simply laid it aside and forgotten it.

One objection to that theory is that none of the employees at the store recalls any package delivered under such circumstances. Another is that, although the retail outlet did have a client whose surname matched the one on the receipt, that person denied ever having received or signed for any package addressed to the complainant. Besides, the first initials were different, and the signatures did not match.

This mystery may never be solved, but at least the complainant was appeased. In the end, our investigator made the delivery to him by hand. Though understandably frustrated by the delay, he was satisfied that the package had been retrieved unopened, its contents intact. He agreed to consider his second complaint settled.

And his third? That came a little later, after he opened the package and took issue with certain exemptions that had been applied to the information. The investigation of the third complaint is still open as we go to press.

Meanwhile, Canada Post assures us that "Lay it aside and forget it" is *not* official policy for mis-addressed packages.

Young Offenders Act: Not all matters of privacy are matters for the federal Privacy Commissioner

It was the first time the Office ever investigated a complaint concerning a young offender's records. It may well be the last. In the end, what our investigation confirmed was that such records are beyond the scope of the *Privacy Act*.

An individual filed a complaint under the federal *Privacy Act* against the Department of Justice. He alleged that the department had denied him access to the Crown's brief relating to the criminal prosecution of a certain youth under the *Young Offenders Act*. The complainant claimed that the youth in question was his "client" (more about that later).

As our investigator discovered, the Department of Justice had only "denied" access in the sense that it had no such information to disclose. The *Young Offenders Act* is indeed a federal law, but it is administered by the provinces. Information of the kind the complainant sought is held not by the federal government, but rather by the respective provincial governments—in this case, Ontario.

On being so informed, the complainant took his information request to the Ontario government, under that province's *Freedom of Information and Protection of Privacy Act*. But the Ontario Attorney General's office responded that the information sought was outside the scope of that act. It further stated, in wording that unfortunately proved misleading to the complainant, that such information was subject to *federal* legislation superseding the provincial act.

What federal legislation did the Attorney General's office mean? The *Young Offenders Act*. What legislation did the complainant take it to mean? The *Privacy Act*. Why hadn't the Attorney General's office been more specific? Because specifying the legislation as the *Young Offenders Act* would in effect have identified the youth as a young offender—identification that the *Young Offenders Act* itself expressly prohibits.

Hence, the complainant pressed the issue under the federal *Privacy Act*, which he mistook for the superseding federal legislation. But the Privacy Commissioner could not help him. As our investigator and several provincial and federal officials eventually agreed, the federal *Privacy Act* does not

supersede the *Young Offenders Act*, which has its own provisions for disclosure of information. Specifically, section 44(1) of that act *does* grant disclosure of a young offender's information, but *does not* give access to parents or representatives once the criminal prosecution has ended. Furthermore, since the provinces administer the *Young Offenders Act*, it is provincial Crown attorneys who determine matters of disclosure under that act.

On the subject of representatives, there is an interesting sideline to this case. Our investigator eventually learned that the complainant had previously followed the proper channel. He had already made an information request under the appropriate legislation, section 44(1) of the *Young Offenders Act*. The local Crown Attorney had denied him access, on grounds that *he was not a competent adult to represent the youth.*

From the beginning, our investigator herself had entertained strong doubts whether the complainant was a bona fide representative of the young offender. Had the case proceeded otherwise, she would have taken steps to confirm the relationship.

As it turned out, representation was beside the point, as far as the Privacy Commissioner was concerned. Given that access to young offenders' information is limited to the *Young Offenders Act* and that such information in any case is not maintained by the federal government, the Commissioner was unable to conclude that any rights had been violated under the *Privacy Act*. The complaint was not well-founded.

Personal information gets trashed–or so Elections Canada hopes

In January of last year, Elections Canada lost a computer tape.

The loss was very troubling to many, for it was not just any old computer tape. This one was full of personal information about most adult residents of Manitoba. More troubling still, it has never been found.

In particular, the tape listed names, addresses, birth dates, and driver's licence numbers of some 675,000 Manitoba motorists. The province's Motor Vehicles Branch had sent the tape by courier for Elections Canada to use in updating voters' lists. In the wrong hands, however, it could be put to any number of inappropriate uses.

The *Canada Elections Act* permits Elections Canada to enter into agreements with various federal, provincial, and territorial agencies for the purpose of obtaining information to update the National Register of Electors. In fact, Elections Canada receives protected data from 27 such sources four times a year. Transferring personal data via computer tape was entirely in keeping with the existing agreement between the Province of Manitoba and the Chief Electoral Officer of Canada.

The loss of the confidential information, of course, was not. The Manitoba agreement, like all others, had been based on the clear understanding that Elections Canada would take every appropriate security and safeguarding measure to protect the confidentiality of the personal information entrusted to it. On learning of Election Canada's failure in this regard, Manitoba's Ministry of Highways and Transportation suspended the information-sharing agreement, pending review of the incident and implementation of satisfactory remedial measures.

Nor could Elections Canada afford to treat its failure lightly. The department greatly depends on information received from outside sources, and both staff and management alike were acutely aware of how severely the incident could affect future dealings with suppliers. From the outset, therefore, Elections Canada spared no effort to restore confidence in its ability to handle and protect personal information.

When five separate, thorough searches of the office complex failed to turn up the missing tape, Elections Canada notified Manitoba officials of the loss and immediately commissioned an independent audit of its own security and data-handling procedures. The department subsequently implemented several recommendations of that audit to improve both the human and technical elements of what had already been a highly sophisticated, albeit obviously flawed, system.

One thing that Elections Canada did *not* do, however, was inform the federal Privacy Commissioner. It was the Ombudsman for the Province of Manitoba who eventually did that— more than two months after the incident had occurred.

Despite the independent audit that had already been carried out, the Commissioner launched his own investigation into the incident. Through on-site inspections and extensive interviews with all employees concerned, Privacy staff confirmed what both Elections Canada and the independent audit had previously concluded about the missing tape:

- It had definitely been received at the offices of Election Canada and been retrieved from the mailroom, as attested by mailroom personnel and others, including the employee who had picked it up.
- It had probably *not* been stolen. The investigation revealed no evidence of theft, by either an employee or an outsider. All employees interviewed proved open, co-operative, and highly credible. Nor was it likely, given the sophisticated security system already in place, that any outsider could have intruded, stolen the tape, and got away undetected.
- In all probability, the tape had been thrown into the trash by mistake. On the day of the incident, the employee who had gone to the mailroom to pick up the tape had other things on his mind. He was worried about his sick infant daughter and, having obtained approval to leave work early, was anxious to go home to attend to her. When he brought the newly arrived tape, in its envelope, to his office, there were five other courier envelopes on his desk. These five had already been emptied of their contents and were awaiting disposal. In his haste and distraction, the employee may well have thrown the new envelope, unopened, into the trash along with the empty ones.
- It was not until three working days later, during a routine audit, that the employee realized the Manitoba tape was missing. By that time, the trash cans of the day in question had long been emptied and their contents removed far from the premises. Because of their wax coating, the courier envelopes would not have been separated for recycling, but rather would have been taken to a landfill site along with other non-recyclable refuse.
- Whatever had become of the tape, it was unlikely that the confidential information could be accessed for improper purposes. There was nothing on the tape cartridge to identify its contents, its origin, or its destination. Moreover, the tape was written in a code unique to IBM mainframe computers and could not be read without special decoding software.

All things considered, the Privacy Commissioner himself concluded that the tape had been lost through simple human error. He found the independent audit report to be very thorough and credible and was satisfied with the remedial measures that Elections Canada had implemented to prevent further breaches of security and confidentiality.

To both the Ombudsman for Manitoba and the Chief Electoral Officer for Canada, the Commissioner conveyed his belief that the tape had ended up buried in a garbage bag at a landfill site.

In other words, it is out of harm's reach—with any luck.

Lax information technology procedures in prison cause a dangerous breach of privacy

When some inmates of a federal prison acquired confidential information on all the others, the consequences, fortunately, were not as dire as they might have been. Since then, Correctional Services Canada (CSC) has made a point of reducing its need to rely so much on good fortune in future.

One of the first steps that CSC took was to report the incident to the Privacy Commissioner. Not all our investigations arise from complaints by private citizens. Sometimes, as in this case, federal departments themselves report incidents warranting the Commissioner's attention.

What CSC reported was that Kingston Penitentiary officials had found, on the hard drive of a computer in an inmate's cell, two spreadsheet files containing information on more than 300 inmates of the penitentiary. The information included not only names and vital dates, but also details of crimes and sentencing, confidential fingerprint sheet numbers, and notations on mental health problems, prison behaviour, and escape risk.

The incident, along with a leaked copy of the spreadsheet files, soon came to the attention of the press. Journalists raised concerns that dissemination of such information could pose danger for some inmates—notably, those identified as sex offenders.

On the day of the incident, penitentiary staff removed the computer and all diskettes from the inmate's cell. The inmate admitted to having received the files on diskette from another inmate several months before and copied them to the computer's hard drive. He also indicated that he knew of other inmates who had the same files.

The next day, staff conducted an "exceptional search" of the institution, seizing all computers and diskettes in the possession of, or otherwise available to, the inmates. This search turned up only one other copy of the files in question.

The next step was to contact all the individuals whose privacy had been breached. After providing the Office of the Privacy Commissioner with a copy of the template, CSC sent appropriate letters of notification to the 333 inmates concerned, informing them of, among other things, their right to complain under the *Privacy Act*. Notifying the inmates was a clear indication

of CSC's acceptance of responsibility for the incident and willingness to take remedial action on a serious matter.

Promising to keep us informed of all developments, the Ontario regional office of the CSC then launched its own investigation into the incident. The following facts emerged:

- The spreadsheets had originally been designed by a penitentiary official.
- More than one staff member had since been involved in updating the information on the files.
- The files were known to have been stored on two computers used by staff: (1) a laptop computer that several staff members had frequently taken home, and (2) a desktop computer that was subsequently loaned out for inmate use. Either or both of these computers could have been the source of the improper information disclosure.
- The laptop computer had gone missing one year before. No monitoring or tracking system for its use had been in place. Therefore, no document trail had been available to assist in finding it.
- When the laptop went missing, CSC had failed to notify the Privacy Commissioner of the personal information on the hard drive.
- Before being loaned out to an inmate, the desktop computer may not have been "sanitized" (i.e., its hard drive expunged of inappropriate files). Although the informatics department usually followed sanitation procedures, the procedure for verification was informal and lax. In this case, there was no documented verification that the computer had been sanitised.

The CSC investigation report concluded that the disclosure of personal information had been caused by procedural breakdown, not by inmates. The report made three strong recommendations towards strict procedural control over equipment loans, computer sanitation, and data storage and security.

We are satisfied with CSC's investigation and believes that, if well implemented, the recommended measures will reduce the likelihood of recurrence. Moreover, the Office considers the actions taken in response to the incident to be positive demonstrations of CSC's continuing commitment to the principles of the *Privacy Act*.

A case about a case, not properly secured

Federal employees who take their work out of the office have no special immunity from thievery. In fact, now that the laptop computer has become a container of choice for transporting office files, employees have to be especially on their guard. A laptop's compact size and high market value make it a very tempting target for thieves.

Last year, when someone stole a small carrying case from an employee's car, the Farm Credit Corporation (FCC) did the right thing by notifying the Privacy Commissioner. The case, which had been locked in the trunk, contained a laptop computer. In the side pocket was a file of papers, disclosing personal loan information on FCC clients.

The FCC conducted a thorough search of the area. The computer was soon found undamaged near a garbage bin not far from where the employee's car was parked. The paper file, however, was not recovered.

The FCC wrote letters to the clients concerned, notifying them of the loss of their personal information. The clients have since acknowledged the loss and seem not to have taken permanent offence. At least, they have agreed to keep doing business with the FCC.

The FCC also sent a memo to all staff, reminding them of the importance of securing personal information. In particular, the memo instructed that

- Client files to be transported should be kept in a locked briefcase in the employee's possession;
- Such files should be returned to the office wherever possible;
- In instances where taking files home is unavoidable, they should be stored in a secured area, preferably in a locked filing cabinet; and
- Any laptop computer taken home should remain with the employee at all times and should not be stored in vehicles or luggage.

In this instance, FCC officials were unable to ascertain whether any personal information had been stored on the computer. In any event, they doubted whether the thieves had either the time or the ability to access any information on the hard drive, particularly since the computer's operating system was protected by a password. From the circumstances of the computer's recovery, the officials thought it likely that the thieves had been foiled in the act.

While generally approving of the FCC's efforts in response to the improper disclosure of information, the Privacy Commissioner felt compelled to raise a concern about security of personal information on portable computers. He stressed that, even though a computer may be stolen for its hardware value, there is always a possibility for information stored on the computer to be used to the disadvantage of individuals to whom the information relates.

As to the FCC's reliance on a mere password to prevent access to a computer's operating system, it is well known that this is not a secure enough measure in itself. Password or no password, a thief could get access to a hard drive simply by using a boot disk.

The FCC's manager of network services operations has acknowledged the need for greater security. In addition to issuing the above-noted instructions to employees, he has informed the Office of the Privacy Commissioner of FCC's plan to equip all of its computers, including laptops, with appropriate software that will protect all data stored on the hard disk.

The Privacy Commissioner urges federal institutions to take every possible precaution for protecting data on portable computers. If you can't prevent a determined thief from stealing the hardware, you can at least make sure he won't get a big bonus in the form of confidential and useful information.

Improper destruction of records: A reprehensible act

When the Privacy Commissioner takes the unusual step of conveying his findings directly to a Deputy Minister, it signifies a matter of great concern to the Commissioner. In this case, unfortunately, the Deputy Minister did not seem to see the matter in quite the same light.

In investigating a complaint against Revenue Canada, our officer made arrangements to visit a regional tax services office. He intended to interview several staff members there and examine all pertinent files and documents. His mission was to determine whether Revenue Canada had granted the complainant all the personal information she had previously requested under the *Privacy Act*. The requested information related mainly to an investigation of a harassment allegation by the complainant.

Before making the visit, our officer spoke with the regional human resources co-ordinator at the site. She told the officer that among the files she had gathered for his review were some hand-written notes of unknown authorship (the author was later identified as the investigator of the above-

mentioned harassment allegation). In the same conversation, the human resources co-ordinator also mentioned her intention to "clean up" the files, mainly by eliminating the many duplicate copies of documents they contained. However, when our officer asked her not to remove duplicates or any other documents before he saw the files, she agreed.

During the on-site visit, our officer could not find the hand-written notes that he had been told to expect. In an effort to find out what had happened to them, he proceeded to interview several of the managers at the tax services office. These interviews revealed that the following events had occurred:

- After speaking with our officer, the human resources co-ordinator had passed the harassment investigation file on to two managers for the purpose of "pulling it together" and making a chronology of events.
- One of these two managers, by his own admission, had subsequently destroyed the hand-written notes of the harassment investigator, in full knowledge that a *Privacy Act* complaint was in progress and that the notes were relevant to an earlier *Privacy Act* complaint.
- The other manager to whom the file had been passed had removed another set of hand-written notes. Without retaining a copy for the file, she had sent this second set of notes to their author, who had been the investigator of a previous harassment allegation by the complainant.

As our investigation later revealed, both sets of hand-written notes referred to certain matters that might reflect badly on local staff in the context of an earlier investigation.

As it happened, neither missing set of notes remained missing for long. For one thing, our officer managed to persuade the author of the second set of notes to return them. For another, and probably unbeknownst to the officials at the tax service office, a copy of the first set of notes was on file at Revenue Canada headquarters in Ottawa. Eventually, Revenue Canada agreed to put both sets back into the harassment investigation file so that they would be duly available to the complainant in future.

Problem resolved? Not quite. There was still the matter of the deliberate removal and destruction of records by officials who should have known better. This was a matter that seriously troubled the Commissioner—so much so in fact that he decided to bring his finding directly to the attention of Revenue Canada's Deputy Minister at that time.

Specifically, the Commissioner raised concerns about the "inappropriate" and "reprehensible" behaviour of Revenue Canada officials, who had contravened both *Privacy Act* retention requirements and their own department's retention and disposal standards. From the evidence, the Commissioner could only conclude that the officials had so acted in an attempt to thwart his Office's investigation.

In response, the Deputy Minister agreed that the improper destruction of personal information was a very serious matter. But he could not agree that his officials' behaviour in this case was reprehensible, since he was satisfied that the "unfortunate incident was neither wilful nor intended to thwart" the Privacy Commissioner's investigation. On what evidence he had become so satisfied, the DM did not venture to say.

He did say, however, that he would remind his officials of the powers and duties of the Privacy Commissioner and of the requirement to fully respect the provisions of the *Privacy Act*.

There is new offence under the *Access to Information Act* (section 67.1) to prevent destruction of records where the destruction is for the purpose of frustrating access to information. Unfortunately, the *Privacy Act* does not contain a similar provision.

Information access: A matter of give and take

When a department is late in responding to an information request, it is not always the department's fault. Sometimes the request itself is unclear, and it takes time for the departmental officials to determine what exactly the requester wants. And sometimes, a requester can save weeks of delay just by picking up the phone.

In one recent case, for example, a man complained that a certain federal department had failed to provide a timely response to his request for information under the *Privacy Act*. He had requested access to all records placed on file since his "last request".

To the departmental ATIP officer who received it, this new request seemed ambiguous. It was her understanding that the requester wanted access to records concerning an internal investigation into harassment allegations he had made against certain departmental officials. However, his new request named some officials who were not parties to that investigation and who were therefore unlikely sources for such records. Furthermore, the man had

made several requests for information in the past, and the *last* one, chronologically speaking, had nothing to do with the investigation in question.

In short, the ATIP officer was genuinely uncertain how she should respond to the new request. She was more than willing to begin responding immediately, but simply did not have clear enough information on which to proceed. After several unsuccessful attempts to reach the man by telephone, she wrote him a letter asking him to clarify what he had meant by his "last request." Specifically, she asked him to quote the file number for it.

On receiving this petition, instead of just telephoning or otherwise dealing with the officer directly, the man for some reason decided to turn the matter over to his legal representative. A full two weeks later, the lawyer wrote to the department, expressing the desire to complain formally about the "excessive delays" in processing his client's information request. This letter was duly forwarded to the Privacy Commissioner and received as a formal complaint under the *Privacy Act*.

But the lawyer's letter also had the effect of adding to the confusion. For the "last request", the letter quoted the file number that the ATIP officer still had good reason to doubt was the right one. In her mind, it was still unclear what records she ought to retrieve.

Section 13(2) of the *Privacy Act* requires that those who request personal records under the Act provide information of sufficient detail to enable the department to make the requested records retrievable. In other words, the onus is on the requester to make sure that his or her request is not ambiguous.

In a lengthy conversation with the lawyer, our investigating officer confirmed what the ATIP officer had suspected: that the records sought were indeed those related to the harassment investigation. Our officer pointed out that the file number the lawyer himself had quoted in his letter of complaint was unrelated to that investigation. In sum, there had been legitimate confusion over what information the complainant was interested in obtaining.

The lawyer finally agreed to close out the matter by forwarding a letter of clarification to the department.

The Commissioner concluded that the department's request for clarification had been valid and that the time-limit complaint was not well-founded.

The SINs of our fathers: At least some of them will not be visited upon us

Hats off to the countless senior citizens who know and cherish their privacy rights.

This is the case of one Quebec woman who grew increasingly annoyed at seeing her confidential Social Insurance Number displayed for anyone to see through the envelope window for her Old Age Security cheques. Deciding finally to do something about it, she complained to the Privacy Commissioner. The final result—we are delighted to report at last—is that neither this senior citizen nor any other will ever again have to suffer that particular violation of privacy rights.

In investigating this complaint, our office could not have been more sympathetic. Why indeed was a Canadian citizen's personal, and supposedly confidential, Social Insurance Number clearly visible through the window of envelopes mailed to her by a federal department? This was not a question we were posing for the first time—far from it. Time and time again we had posed it, in the course of investigating many a similar well-founded complaint, dating as far back as 1986.

By now the question had become more pointed: After many years of being repeatedly shown the error of its ways, repeatedly acknowledging the error, and repeatedly making promises to eliminate it, why was Human Resources Development Canada *still* disclosing confidential information by public post in outright contravention of the *Privacy Act*?

To give the department its due, this time the response was different—no more empty promises, no more "next year for sure", no more tyranny of "systems", no more halfway measures. The department not only said it would remove, but actually did remove, SIN from its Old Age Security cheques, as of November 1, 1999.

Small victory though it may seem, it could not have happened without the persistent indignation of senior citizens such as the complainant from Quebec. Perhaps because it understands best the integral relation between liberty and privacy, the older generation tends not to suffer quietly even the smallest violations of either. The big question arises: will younger generations be willing to take up the torch?

Partial remission of SIN: a fair compromise, albeit another dubious pun

Even if it doesn't show through its envelope window, a Social Insurance Number (SIN) printed on a government-issued cheque does not stay hidden forever. Sooner or later the envelope gets opened, and the SIN becomes visible to people who really have no right to see it—notably, the people who cash the cheque.

Down through the years, the Commissioner has received many complaints to that effect. When he received one recently from a northern counterpart of his, the special circumstances of the North made all the difference.

The Information and Privacy Commissioner for the Northwest Territories complained that Human Resources Development Canada (HRDC) was making improper disclosures of SINs by printing them on cheques for employment insurance benefits. Her contention was that recipients therefore cannot cash their cheques without revealing personal information to a financial institution or other cheque-cashing establishment.

HRDC still prints the SIN on several kinds of cheques it issues. Of these, employment insurance cheques are the case for which the department offers perhaps its best argument. In this instance, as often in the past, HRDC explained its position as follows:

- Given that the SIN was designed for employment insurance purposes in the first place, its use on employment insurance cheques is entirely appropriate and legitimate. Furthermore, the SIN is the official file number for the employment insurance program, and as such is an important element in establishing the identity of cheque recipients. Since many persons may have the same name, an employment insurance payment is actually issued not to a name, but rather to a SIN.
- In cases where a cheque was lost or stolen, tracing it would be expensive and laborious without the SIN.
- As far as confidentiality is concerned, financial institutions already have responsibility for recording the confidential SIN for certain other transactions. Establishments other than financial institutions may not have similar SIN responsibilities, but on the other hand people who have their cheques cashed at such alternative establishments do so by their own choice.

- Another good option available to recipients is having their cheques deposited directly into their bank accounts. Direct deposit obviates the need for any others to cast their eyes upon the confidential SIN.

The Office sees some merit in the HRDC argument, particularly as it relates to the options generally available to cheque recipients. Financial institutions do indeed already have routine access to SIN, notably for transactions such as reporting income to Revenue Canada. Presumably, they also have safeguards in place for the protection of this personal information. Likewise, it is true that direct deposit may bring a greater measure of privacy.

However, when the Northwest Territories come into the picture, the HRDC position weakens. In the many sparsely populated areas of Canada's North, financial institutions may be few and far between. Direct deposit or no direct deposit, it's hard enough just to get to the bank. Many northerners have to rely on whatever alternative cheque-cashing facilities may be available—the local general store, for example.

Such establishments may have attractions of their own, of course, but they are not known for the kind of anonymity that one often seeks in a financial institution. After all, it is one thing to have your SIN scanned by an unknown and indifferent bank teller, but quite another to be obliged to disclose personal information to a friend, relative, neighbour, or local acquaintance.

The Office is pleased to announce that, as a result of discussions arising directly from this northern complaint, HRDC has softened its line. It has agreed to examine its use of social insurance numbers on the cheques it issues—not just for employment insurance, but for *all* of its programs. More concretely, the department has already proposed to change its procedures so as to print not the whole SIN but rather only the last six digits on each cheque it issues.

Would six digits be enough for HRDC? Yes. The department has conceded that six digits are all it really needs for most purposes of identification.

But would merely eliminating three digits of the SIN be enough to address the privacy issue? In good part, it would. For one thing, the six remaining digits would not be identified as part of a SIN, nor would they be recognisable as such. For another, no one, not even HRDC, could guess or recreate the complete SIN from the last six digits.

In short, both the federal commissioner and the territorial commissioner regard this proposal as a reasonable compromise. While acknowledging that

the change may not be accomplished overnight, the Privacy Commissioner has assured his northern counterpart that he will monitor the progress of HRDC's undertaking.

Inquiries

After the brief levelling-off period last reported, inquiries went over the top again this year. Our two-person inquiries unit processed some 11,256 calls and letters in 1999/2000. This exceeds last year's total by 953 and the previous high in 1997/98 by 925.

The table below shows received inquiries broken down into broad categories.

Inquiries by Type
for the year ended March 31, 2000

Adoption, genealogy, missing persons	83
Criminal records, pardons, U.S. waivers	130
Financial institutions, insurance, credit bureaus	367
Medical	121
No jurisdiction, private sector	780
No jurisdiction, federal	805
Other	698
Privacy Act, interpretation & process	4364
Public Affairs (media, publications)	1036
Redirect to provincial commissioner	794
Redirect to other federal agency	686
Redirect to other	135
Social Insurance Numbers	1099
Telecommunications	75
Telemarketing, direct mail	83
Total	**11256**

Of special interest

Public Information: More callers than ever reported difficulties in finding Personal Information Request Forms and copies of *Info Source*, the catalogue of the federal government's information holdings. Under the *Privacy Act*, the Treasury Board Secretariat is responsible for producing these materials and making them available at post offices, libraries, and other public places. But Treasury Board appears to have become less and less diligent about carrying out this responsibility—at least as far as distribution is concerned. According to our callers, not only do many post offices not have these materials on hand, but also some postal employees, particularly at the smaller retail outlets, are not even aware that such things exist.

Furthermore, even when people do find copies of *Info Source*, they seldom like what they see. The document itself provokes many calls of dissatisfaction to our inquiries unit. Frustrated callers say that *Info Source* is too big and unwieldy, too dauntingly technical, too difficult to read and find one's way around in—in short, not nearly as helpful and user-friendly as it should be for the ordinary Canadian citizen. Frankly, from our own almost daily experience with the document, we can only agree. The directory of the federal government's information sources should be less a compendium and more a guide for the average user.

The Office would like to assist in improving *Info Source* and in fact has already initiated discussions with Treasury Board to that end.

Social Insurance Numbers: Once again, the SIN was on the mind of many inquirers. This year's SIN-related inquiries exceeded even last year's total, which had burgeoned as a result of commentary by the Auditor General. In fact, more than 40 per cent of telephone inquiries in 1999/2000 related to the use of the SIN.

Electronic Surveillance: Many callers asked about the legalities of various forms of electronic surveillance, notably hidden cameras and monitoring of telephone calls and computer use. Callers included both employees under surveillance and employers contemplating possibilities for their workplaces.

Post-1911 Census Information: Inquiries continued to be made about the release of census results of 1911 and subsequent years. In large part, these inquiries have been prompted by the Privacy Commissioner's expressed opposition to releasing information that the government originally promised to keep confidential.

Statistics Canada: The Labour Force Survey prompted numerous complaints

about Statistics Canada. Many complained of harassment by StatsCan agents. It is expected that the next big survey of 2001 will bring a new flurry of inquiries relating to the behaviour of canvassers and to the question of citizens' obligation to participate.

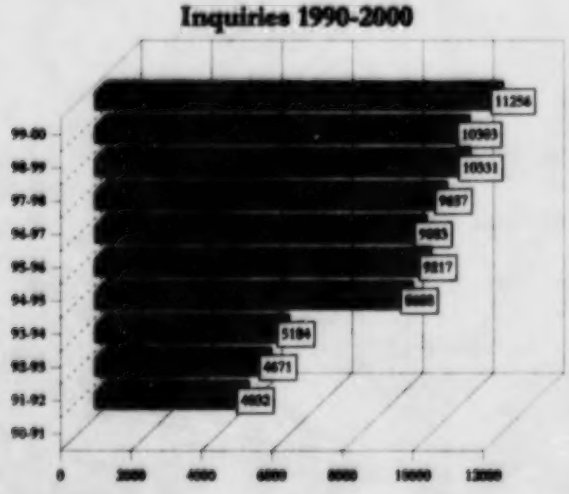
Private Sector: Every year, our staff fields large numbers of inquiries concerning private-sector companies and institutions. This year, for example, many continued to report dissatisfaction with the complaint process at financial institutions. Others alleged that credit reporting agencies were providing false or inaccurate information about them, or that collection agencies were harassing them and disclosing personal information to third parties. Several calls came from private-sector employees who were trying to gain access to their personnel files. These callers were invariably dismayed to learn that there is not yet any legislation in place that permits such access.

To date, with only the *Privacy Act* to guide us, we have been limited in what we could do for such inquirers. With the passage of Bill C-6, we hope to be much more helpful in the future.

During the Commissioner's Term

In 10 years since taking office, Commissioner Phillips saw the number of annual inquiries increase between two- and threefold, from 4,032 in 1990/1991 to 11,256 in 1999/2000. The average annual increase was just under 10 per cent, for a grand total of 82,422.

The table below shows totals for each of the Commissioner's 10 years in office.



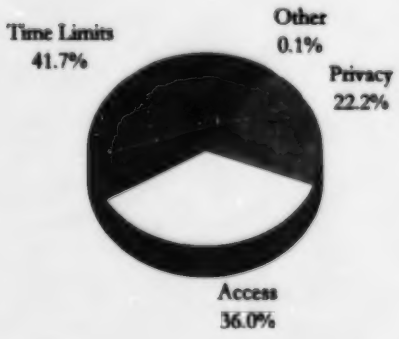
Top Ten Departments by Complaints Received

for the year ended March 31, 2000

	Total	Access	Time	Privacy	Other
Correctional Service Canada	**316**	109	136	71	
Revenue Canada (Now Canada Customs and Revenue Agency)	**231**	103	81	47	
National Defence	**189**	53	91	45	
Royal Canadian Mounted Police	**130**	67	37	26	
Human Resources Development Canada	**120**	35	16	69	
Immigration and Refugee Board	**108**	8	92	8	
Citizenship and Immigration Canada	**72**	32	29	11	
Justice Canada	**64**	52	3	9	
Canadian Security Intelligence Service	**58**	53	3	2	
Canada Post Corporation	**38**	10	3	25	
Other	**260**	124	66	69	1
Total	**1586**	**646**	**557**	**382**	**1**

Closed Investigations by Grounds

Fiscal Year 1999-2000



Completed Investigations by Department and Result

for the year ended March 31, 2000

Department	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	4	0	0	0	0	1	5
Atlantic Canada Opportunities Agency	0	0	1	1	0	0	2
Business Development Bank of Canada	0	0	0	0	0	1	1
Canada Ports Corporation	1	1	0	0	0	1	3
Canada Post Corporation	6	1	7	6	1	15	36
Canadian Heritage	2	0	2	0	1	1	6
Canadian Human Rights Commission	0	0	0	0	0	1	1
Canadian Museum of Civilization	0	0	0	0	0	1	1
Canadian Radio-television & Telecom. Commission	0	0	1	0	0	0	1
Canadian Security Intelligence Service	3	0	15	0	0	18	36
Canadian Space Agency	0	1	3	0	0	0	4
Citizenship and Immigration Canada	41	8	10	4	1	11	75
Correctional Service	149	13	71	15	7	45	300
Environment Canada	0	0	2	0	0	0	2
Farm Credit Corporation	0	0	0	1	0	0	1
Fisheries and Oceans	0	0	1	0	0	0	1
Foreign Affairs and Int. Trade Canada	4	0	4	0	0	2	10
Health Canada	4	1	6	4	1	2	18
Human Resources Dev.	14	3	21	9	2	50	99
Immigration and Refugee	90	15	11	1	0	0	117
Indian and Northern Affairs Canada	2	1	1	0	0	1	5
Subtotal	318	43	155	41	13	149	719

Department	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Industry Canada	1	0	0	0	0	0	1
Inspector General of the CSIS	0	0	0	0	2	0	2
Justice Canada,	1	3	15	2	1	14	36
National Archives of Canada	3	3	4	0	0	7	17
National Defence	107	10	43	5	3	28	196
National Parole Board	1	4	10	1	4	3	23
National Research Council Canada	0	0	1	0	0	0	1
Natural Resources Canada	2	0	3	2	0	1	8
Office of the Chief Electoral Officer	0	0	0	0	1	0	1
Pension Appeals Board	0	0	0	0	0	1	1
Privy Council Office	0	0	3	0	1	1	5
Public Service Commission of Canada	12	1	0	1	0	4	18
Public Service Staff Relations Board	0	0	1	0	0	0	1
Public Works and Govt. Services	11	2	6	0	0	5	24
RCMP Public Complaints Commission	0	0	0	0	0	3	3
Revenue Canada (Now Canada Customs and Revenue Agency)	93	8	41	6	4	28	180
Royal Canadian Mounted Police	19	3	42	8	3	31	106
Solicitor General Canada	0	1	13	0	0	1	15
Statistics Canada	0	0	0	3	0	0	3
Transport Canada	7	1	2	2	0	1	13
Treasury Board of Canada	0	0	3	0	0	0	3
Veterans Affairs Canada	5	1	5	1	1	5	18
Total	**582**	**81**	**348**	**72**	**33**	**283**	**1399**

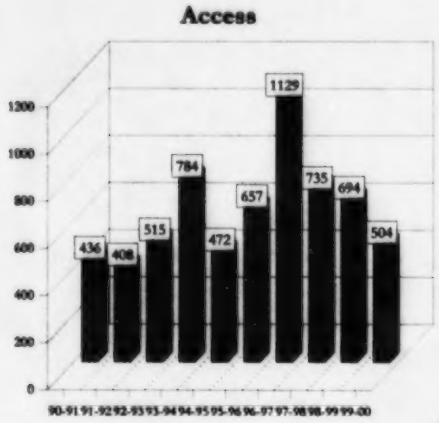
Origin of Completed Investigations

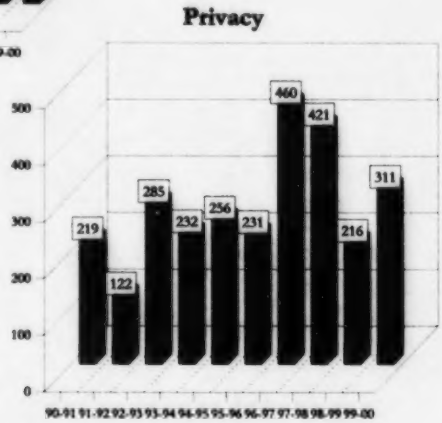
for the year ended March 31, 2000

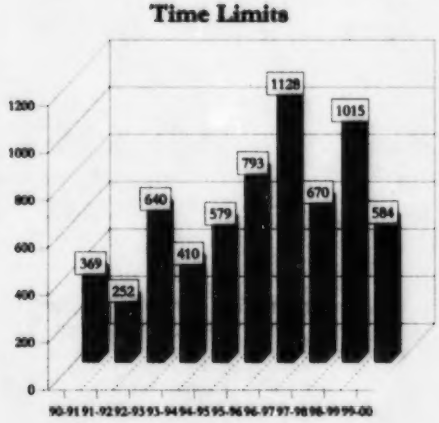
Newfoundland	3
Prince Edward Island	6
Nova Scotia	43
New Brunswick	45
Quebec	337
National Capital Region - Quebec	9
National Capital Region - Ontario	192
Ontario	327
Manitoba	72
Saskatchewan	40
Alberta	85
British Columbia	229
Northwest Territories	1
Yukon	2
Outside Canada	8
Total	**1399**

Completed Investigations by Type

for the last 10 years







In the Courts

Ten years of significant court decisions

After 10 years in office, it seems appropriate to consider some of the lessons learned from the Courts over the past 10 years. The following interpretations are based on those court decisions listed at the end of this section.

Access to personal information

- Heads of a federal government institution who receive requests for disclosure of personal information under the public interest provisions of the *Privacy Act*, must consider the matter, by weighing the public interest in disclosure against any invasion of privacy that could result from the disclosure. If the head has exercised discretion properly, the Court will not overturn the decision (C).
- Information about government positions (e.g., security classification, occupational group and level or language requirements) is not "personal" even if it incidentally reveals something about employees in these positions (C & I). However, information particular to these employees (vacation credits, health or performance appraisals) is "personal" (C & J).
- An individual's right to access his/her information is not absolute when it is so intertwined with another's information that disclosure would reveal personal information about someone else (D).
- All parties involved in administrative investigations (grievances or harassment complaints) should have access to all the information used to reach a finding. This is a compatible use disclosure under the *Privacy Act* and meets the requirements of natural justice (F).

Control over personal information

- All information in the hands of a federal government institution is subject to the *Privacy Act* (except that which is expressly excluded from it). The act does not indicate that this control can be diminished or abandoned by contracting with a third party (G).

Relationship between the Privacy Act and the Access to Information Act

- The *Privacy Act* has equal status with the *Access to Information Act* and must be given equal attention when dealing with government information. However, if this information is "personal" as defined in section 3 of the

Privacy Act, privacy protection becomes paramount over access to the information (C).

Solicitor-client privilege

- The right to waive the protection of confidential communications between lawyer and client—solicitor-client privilege—belongs to the client, not the lawyer (A).
- Waiving the solicitor-client privilege over part of a document does not automatically require disclosing the rest of the document. However, the entire document could lose its protection if a selective disclosure misleads the person receiving it (B).
- A detailed breakdown of a lawyer's bill is protected by solicitor-client privilege because it can reveal the nature of the work the lawyer performed (B).
- As the *Privacy Act* does not define "solicitor-client privilege", the common law serves as the guide (H).
- When heads of federal institutions refuse to disclose information because it is protected by solicitor-client privilege, they must demonstrate that each document was prepared either as legal advice or predominantly for litigation (H).
- In order for the head of a federal institution to refuse to disclose confidential communications between lawyer and client, the head must confirm that the communications are indeed protected and that the client is not willing to give up this protection (E).

Court decisions referred to above:

A. R. v. Campbell [1999] S C.R. 565;

B. Stevens v. Canada (Privy Council) [1997] 144 D.L.R. (4th) 553;

C. Michael A. Dagg v. The Minister of Finance [1997] 2 S.C.R.403;

D. Mislan v. The Minister of Revenue Canada, T-2790-96, decision dated May 22, 1998, F.C.T.D., not reported;

E. Canadian Jewish Congress v. Canada (Minister of Employment and Immigration) [1996] 1 F.C. 268;

F. Puccini v. Canada (Director General, Corporate Administrative Services, Agriculture Canada), [1993] 3 F.C. 557 (T.D);

G. Canada Post Corp. v. Canada (Minister of Public Works), [1993] 3 F.C. 320 (T.D.)-Affirmed in (1993), 64 F.T.R. 62 (F.C.A.);

H. Weiler v. Canada (Minister of Justice) [1991] 3 F.C. 617 (T.D);

I. Information Commissioner v. Secretary of State for External Affairs [1990] 1 F.C. 395;

J. Information Commissioner of Canada v. Solicitor General of Canada [1988] 3 F.C.551.

Ongoing cases

1. Privacy Commissioner v. Attorney General (Court file: A-121-99)

2. The E-311 form (Court file: A-401-99)

Both these cases challenged Human Resources Development Canada's (HRDC) collection of returning travellers' customs declarations to police the unemployment insurance program. In the first case, HRDC appealed the decision of Justice Tremblay-Lamer on the interpretation of section 108(1)(b) of the *Customs Act* which delegates to the Minister the right to approve the release of information, and interpretation of section 8(2) of the *Privacy Act*. The Court of Appeal's decisions were delivered on February 9, 2000.

Justice Tremblay-Lamer found that the Minister of National Revenue's blanket authorization for disclosure of the customs declarations on July 26, 1991, was an invalid exercise of discretion and an unlawful obstacle on the future exercise of discretion, and was based on irrelevant considerations. However, according to the Court of Appeal "[t]he issue before [the judge] was not however with respect to that blanket authorization, but to 'the Ancillary Memorandum of Understanding for data capture and release of customs information on travellers' entered into on April 26, 1997 by National Revenue, on one hand, and the Canada Employment Insurance Commission, on the other hand." The Court of Appeal concluded that the 1997 Ancillary Memorandum was an authorization of its own, independent from that given in 1991.

The appeal court considered that section 8(2)(b) of the *Privacy Act* (which allows personal information to be disclosed in accordance with another act of Parliament or regulations) is to be interpreted largely: "In this context, paragraph 8(2)(b) cannot but be interpreted as being a provision that enables Parliament to confer on any Minister (for example) through a given statute a wide discretion, both as to form and substance, with respect to the disclosure

of information his department has collected, such discretion, of course, to be exercised in conformity with the purpose of the *Privacy Act*."

The government met its privacy obligations, the appeal court concluded, because "the Minister satisfied herself that the disclosure sought by the Commission was for a permissible use and that no more information than that needed by the Commission would be disclosed." As well, the April 1997 Ancillary Memorandum of Understanding restricted the use of the information and its disclosure to third parties, established an audit trail and provided for destruction of that information.

The second case examined whether UI claimants and other Canadians have a reasonable expectation of privacy in their information on customs form (E-311) that would trigger section 8 of the *Canadian Charter of Rights and Freedoms*. It also considered whether section 32(b) of the *Unemployment Insurance Act* offended the freedom of movement guarantee under section 6(1) of the *Charter*. The Court rejected both arguments.

The Privacy Commissioner will ask the Supreme Court of Canada for permission to appeal both these decisions. If the Court of Appeal's interpretation of section 8(2)(b) is correct, then this provision of the *Privacy Act* offers Canadians no protection against government institutions' sharing their personal information when a statute provides ministers blanket authority to disclose information. No matter how broad or imprecise section 108 of the *Customs Act* may be, it, and similar provisions in other laws, will supersede the *Privacy Act*.

The Commissioner believes that electronic rummaging through government files makes a mockery of Charter protection against unreasonable search or seizure, and of the presumption of innocence—particularly when the search is based on no reasonable grounds for suspicion, and subject to no independent review. Should these data matches become routine, government will no longer protect any of its citizens' personal information against access (except in specific circumstances set out in the law), no matter whether the information was freely given or compelled by law. If section 8(2)(b) is merely a sieve for passage of any government disclosures, and the Charter provides no protection against this type of data matching, then nothing prevents government assembling and circulating huge databases of personal information among federal agencies—and possibly beyond.

Like most privacy laws around the world, the *Privacy Act* includes fair information practices that limit the collection of personal information and restrict the use and disclosure of that information to those purposes stated at

the time of collection. Exceptions to such limits (such as section 8(2) of the *Privacy Act*) must be as few in number and as narrow in scope as possible. In the Privacy Commissioner's opinion, the above decision broadens the scope of section 8(2) of the act to the point where the protections afforded by the act are rendered meaningless.

- Privacy Commissioner of Canada (Appellant) v. CLRB (Respondent) (Court file: A-685-96)

As reported in our 1996-97 annual report (page 40), the Privacy Commissioner has appealed the decision. May 9, 2000 has been set for the Court of Appeal hearing.

- The Office of the Commissioner of Official Languages (Appellant) and Robert Lavigne (Respondent) and the Office of the Privacy Commissioner of Canada (Intervenor). (Court file: A-678-98)

As reported in last year's annual report (page 84), the OCOL has appealed the decision but the Court of Appeal is heavily booked. A hearing date is not expected until at least September 2000.

Complementing C-6: Private Sector Initiatives

Reclaiming your internet privacy: technology to the rescue!

Readers of previous annual reports may remember our lamenting the erosion of privacy over the Internet: insecure electronic mail, pervasive cookies, old postings coming back to haunt us—the list was long and getting longer every year. The Internet is no longer the academic information exchange forum it once was; it has now resolutely entered the commercial mainstream. Almost every site owner on the World Wide Web is intent on making that presence profitable, and this means new and more inventive strategies to attract, retain, track, study, target, and sometimes discard or reject surfers.

Until recently, cyber-visitors knew little—if anything— about the ways Web sites and advertisers could track and monitor their on-line movements. But growing media interest in "e-commerce" and hacker pranks, have made both experienced and potential Web surfers more cautious about providing personal information over the Internet. (See the results of the EKOS survey discussed earlier in this report.) This has also led some companies to develop and exploit a promising market for privacy-enhancing products for the Internet. Some are computer-based, meaning they must be installed on your computer. Others are Web-based, and can be downloaded from the Internet. Some of these technologies are discussed below.

We have long argued that when it comes to controlling the collection and use of personal information, there is no substitute for effective privacy protection laws, which Bill C-6 will provide. But just as people supplement the protection of law with locks to protect their property and self-defence courses to protect themselves, people can use technology to provide an additional layer of privacy protection on the Internet. Of course, these products cannot replace user vigilance, but they can certainly reassure privacy-conscious surfers.

Surfing, chat and news groups

One of these privacy products is Zero Knowledge's Freedom commercial computer-based software, released recently. Freedom enables any Internet aficionado to surf the Web under a variety of assumed names (a *nom de Net*, if you like)—for example, one for real estate sites, another for cancer research sites, and a third for horseracing sites. While a Web site can still track the assumed name and even send it a cookie, the site owners will never know who is behind the name MadMom or BigBang. And Freedom subscribers can also use assumed names when participating in chat or news groups. SiegeSoft has just released a similar but Web-based product.

But anonymizing software is not new: the well-known commercial site of The Anonymizer has been offering users the possibility to surf the Web and subscribe to news groups anonymously for several years. Privada Inc also offers commercial anonymous Web surfing but, unlike Zero Knowledge and The Anonymizer, the company can link an alias to someone's real identity if asked—for example, by a law enforcement agency. PrivacyX launched its competing anonymous surfing and e-mail service in September 1999 but cancelled the surfing feature a few days later because of a software flaw.

In October 1999, Eponymous began offering Web surfers a free utility that segregates information about surfers' identities from other personal data such as age, gender, interests and appetites. The company also warns surfers about a site's data handling practices. When a site presents a registration form, the utility will only release non-identifying personal information. Lucent Technologies also released its free Proxymate utility in October, letting users block information that typically gets sent to Web sites, and creates aliases for site registration.

E-mail

Anonymous remailers forward your e-mail to its destination after removing any information that could trace it back to you. But remailers can be forced to turn over identities of some of their clients. There have been allegations that government or law enforcement agencies actually run some remailers. The best alternative to remailers is encryption—the more bits in the encryption keys, the better—and slower.

Phil Zimmerman's Pretty Good Privacy software, now distributed by Network Associates, is a well known computer-based e-mail encryption software, although some may find it too complex. Zero Knowledge's computer-based *Freedom* allows its subscribers to send and receive untraceable, encrypted e-mail (using 2048-bit keys) through a series of computers located around the world.

Despite the untimely cancellation of its anonymous Web surfing product, PrivacyX still offers its anonymous e-mail service to subscribers. ZipLip provides Web-based encrypted e-mail (using 128-bit keys) that covers your tracks by automatically "shredding" messages after they have been read. More flexible but on the same principle, Global Market's 1 on 1 software offers encrypted email (using 2048-bit keys) and allows users to specify the date on which a message should be deleted. (The message is never actually deleted: the decryption password attached to the message ceases to be valid.) For even greater flexibility, QVtech's Interosa service allows someone to send an encrypted e-mail message and control several aspects of its use, including to whom it can be forwarded and whether it can be printed, edited or copied. The message can also be erased from the Interosa server after a specified date.

Rounding off the list of Internet privacy-enhancing technologies, HushMail is a free, fully encrypted Web-based e-mail service (using 1024-bit keys). Lastly, Tumbleweed Communications Inc.'s product enables an e-mail recipient to go to a sender's site to view or retrieve an encrypted message or document through a secure Web page to which only the recipient has access.

Marketing to children: The Canadian Marketing Association's guidelines

The Office of the Privacy Commissioner has, for several years, advocated legislation to protect Canadians' privacy rights when dealing with the private sector. As much as we welcome Bill C-6, we recognize the value of other complementary measures. Just as we see a place for consumer vigilance and privacy-enhancing technologies (see the previous article) we also see an important role for industry-led efforts to promote and protect privacy.

The Canadian Marketing Association (CMA) has an enviable record of voluntarily safeguarding consumer privacy. The CMA was one of the first major industry associations in Canada to require its members to adhere to a privacy code. And it was the first to call on the federal government to legislate consumer privacy protection in the private sector. Last year marked another CMA first—guidelines on marketing to children. The guidelines can be found in the CMA's *Code of Ethics and Standards of Practice* (the CMA Code) under "Special Considerations in Marketing to Children."

When marketing to children (anyone under the age of 13) marketers are required to observe the following principles

- Marketers must use "marketing techniques that are appropriate to

children." This includes using language a child would readily understand. It also implies refraining from using any practice that could be construed as exploiting "children's credulity, lack of experience or sense of loyalty";

- Marketers must obtain the "express consent" of a child's parent or guardian before collecting, retaining or transferring a child's personal information; and
- Marketers shall not accept an order from a child without a parent or guardian's express consent.

CMA's guidelines are particularly welcome and timely as children go on-line. Children are particularly receptive to marketing techniques, and hence vulnerable to exploitation for commercial ends. Stories abound of children unwittingly disclosing information about themselves and other family members to irresponsible and unethical marketers.

The CMA guidelines do not specify how these principles are to be applied in the "virtual marketplace". It is not clear how a marketer will determine the age of an individual responding to its solicitation, or confirm a young person's age. It will be equally difficult to verify the authenticity of the person claiming to be the child's parent or guardian. These are some of the problems that American e-mail services and websites are wrestling with in attempting to comply with the U.S. *Children's Online Privacy Protection Act*, which requires marketers to obtain parental consent before collecting, using or disclosing personal information from a child.

The CMA Code provides that, when marketers collect personal information that will be linked with "clickstream" data from a visit to a website, they must advise consumers what information is being collected and how it will be used. Marketers must also give consumers a "meaningful opportunity" to decline to have this information collected, or disclosed for marketing purposes. The CMA Code puts the onus on consumers to exercise their right to suppress identifying information. This is unreasonable, particularly when dealing with children.

Ultimately the CMA sees education as the best defence against abuse of children on the Internet. Parents and care-givers may want to review the CMA's publication, *Protecting Children's Privacy: Tips for Parents* at http://www.the-cma.org and Media Awareness Network's *Privacy Playground* at http://www.media-awareness.ca.

Privacy Update

The provinces and territories

Alberta

In 1999, the provincial *Freedom of Information and Protection of Privacy Act* was extended to municipalities and police commissions. The provincial legislature also passed a new *Health Information Act* (reviewed in another section of this annual report), which is not yet in force.

In May 1999, provincial Information and Privacy Commissioner Robert Clark ruled that Statistics Canada's Survey of Financial Security was an unreasonable invasion of an individual's privacy. This led to Statistics Canada changing its approach for a subsequent Household Spending Survey, seeking prior guidance from the Commissioner's office and clearly advising respondents that the survey was voluntary. The Commissioner is also actively pursuing an outreach program in schools and colleges to educate young Albertans on their privacy rights.

British Columbia

Mr. David Loukidelis was appointed the new provincial Information and Privacy Commissioner, succeeding Dr. David Flaherty at the end of his term. Mr. Loukidelis, a lawyer, was a founding member of the British Columbia Freedom of Information and Privacy Association and the main author of its law reform report that played a key role in enacting the provincial *Freedom of Information and Protection of Privacy Act.*

The provincial legislature, acting on the recommendation of its special legislative committee that reviewed the act, has struck a special committee to explore options for privacy protection in British Columbia's private sector. The committee is currently holding public hearings and accepting submissions to determine how the province can best meet its citizens' privacy needs.

The public sector issue of greatest concern to the B.C. Commissioner's Office is the proliferation of video surveillance systems, such as those proposed for law enforcement in Kelowna and Vancouver. The Office considers that video surveillance should be adopted only if there is a compelling and overwhelming case in each proposed location, and if surveillance is the only viable and effective means of deterring and detecting illegal activity. The Office plans to monitor the Kelowna and Vancouver systems if they are built, both to ensure their compliance with the provincial *Freedom of Information and Protection of Privacy Act* and to prevent the unauthorized collection of personal information.

Manitoba

The Manitoba Ombudsman's Office has seen a steady increase in the number of complaints received since the proclamation of the *Personal Health Information Act* (December 1997) and the *Freedom of Information and Protection of Privacy Act* (May 1998). The Office issued its first special report under the acts, *A Privacy Snapshot... Taken September 1999*, to contribute to a greater public awareness and discussion of the privacy issues that confront Manitobans. The Office also began working on two performance-based analytical tools to help it review compliance with the legislation: a privacy impact assessment, and an access practices assessment. Beta tests of these tools should be completed in 2000. The Office will launch its Web site in the spring of 2000 as part of its statutory duty to inform the public about the provincial access and privacy legislation.

Beginning in April 2000, Manitoba's local public bodies (educational, health care and municipal government organisations) will be covered by the *Freedom of Information and Protection of Privacy Act*, bringing this statute into full force.

Ontario

The provincial Ministry of Health's long proposed, and long delayed, *Personal Health Information Protection* legislation appears to be undergoing further revisions. It may yet be further postponed if the government considers integrating it into new provincial private sector legislation, in response to the federal government's private sector privacy bill.

Another initiative with significant privacy implications is a new multi-purpose government smart card, announced in the fall 1999 Throne Speech. Ontario's Information and Privacy Commissioner immediately contacted the provincial government, which has committed to full and open consultations with the Commissioner throughout the project.

On another front, the Commissioner has participated in work groups led by the Ministry of Transportation to help build privacy safeguards into the province's Red Light Camera initiative (meant to deter people from driving through red lights). Also on the justice theme, the Commissioner has been working with the Ministry of the Attorney General on access and privacy issues relating to the provincial Integrated Justice project (aiming at linking law enforcement and court data). The Commissioner has also begun work with the U.S. Department of Justice to develop privacy design principles for integrated justice systems.

The Commissioner was also consulted and offered comment on the provincial Management Board Secretariat's new Privacy Impact Assessment Guidelines.

Québec

The provincial Access to Information Commission has published a teaching tool titled *Infoway – Caution: School Zone.* This guide targets Québec primary and secondary school children that use Internet, advising them on how to surf the Web safely. The guide also gives safe surfing parameters to teachers and school principals, who are urged to design procedures and sites that will protect the children. Lastly, the guide helps parents better understand the privacy impact of new technologies.

The Commission has analyzed an information sharing agreement between the provincial Revenue Ministry and a private polling firm tasked with assessing the effectiveness of its alimony enforcement program. The Commission ruled that the Ministry breached both its enabling legislation and the provincial public sector privacy protection statute. The Ministry was then ordered to retrieve and destroy all of its information from the private polling firm, as well as information collected by the firm during the assessment. Following this intervention, the Commission published minimal requirements for all provincial government agencies conducting polls either directly or through private companies.

Lastly, the Commission has implemented its new hearing process for complaints that cannot be mediated. As of January 31, 2000, the Commission had heard more than 25 such complaints.

Saskatchewan

Mr. Gerry Gerrand has been named the new provincial Information and Privacy Commissioner at the end of Mr. Derrill McLeod's term. Mr. Gerrand is with the law firm of Gerrand, Roth, Johnson and is also the provincial Conflict of Interest Commissioner.

Privacy around the world

Australia: is the phoenix rising again?

Australia seemed poised to enact a federal private sector privacy law in the mid 1990s. However, that project died in 1997 after the then-Prime Minister failed to follow through on a campaign promise, overruling his Attorney General's recommendation to pass such a statute. The government then encouraged businesses to self-regulate, a move denounced by consumer and privacy advocates who managed to keep the issue alive.

To help businesses regulate themselves, the Australian Privacy Commissioner developed eight privacy protection principles based on the 1980 Guidelines of the Organisation for Economic Co-operation and Development. Some Australian states, however, continued to push their own private sector privacy protection agenda. Australian businesses began to fear the patchwork of standards that could emerge if the federal government refused to act. They were also concerned that without a law Australia could suffer once the European Union implemented its Directive on data protection.

Once again the Australian government has promised to introduce a federal private sector privacy protection law. That law, however, would be based on the Privacy Commissioner's eight principles which the Australian Senate's Legal and Constitutional References Committee described as "weak and piecemeal" and having "serious deficiencies". The Australian law would recognize self-regulatory privacy codes, backed by the above principles, and approved and overseen by the Privacy Commissioner. If a company or industry failed to develop a code, the law's complaint-handling regime administered by the Privacy Commissioner would apply.

On November 30, 1999, the Australian Attorney General announced his intention to seek further public comments over the next few months, and to table the draft law in 2000.

European Directive: a thorn in the American side

The European Union's Directive on data protection came into force in October 1998, meaning member countries could no longer give their citizens' personal information to non-member countries that do not adequately protect the information. This includes Canada and the United States of America—although Canada will probably meet the EU test now that Parliament has passed Bill C-6. The USA have had a *Privacy Act* in force since 1974 but it applies only to federal government agencies (much like the current Canadian *Privacy Act*). The American private sector is currently unregulated and

insists on keeping it that way; fearing state interference and believing that privacy regulation would be an unnecessary burden that would stifle free enterprise. In an attempt to avert a transatlantic trade war with one of Europe's major trading partners, EU officials agreed to negotiate with their American counterparts to reach a mutually agreeable solution.

Last year's annual report described the American proposal to establish "safe harbours". If accepted, the EU would consider American companies (rather than the country) as providing "adequate" protection if they comply with a set of voluntary data protection principles. These principles would require the company to describe for clients how it handles and shares their personal information. EU officials did not reject the American proposal but sought two additional guarantees: their citizens should be able to access whatever information an American company has about them, and there should be adequate and accessible mechanisms for EU citizens to enforce compliance. Of course, the American enforcement route is through the courts (a long and costly process). EU countries enforce data protection rules with independent Commissioners who are empowered to order remedial action at no cost to the citizens.

Talks between the two sides broke down in December 1998. A first deadline of April 30, 1999, came and went without agreement, perhaps caused in part by American companies' lack of support for their government's Department of Commerce "safe harbour" proposal. These companies are worried that the proposal could lead eventually to the USA adopting national privacy legislation, a move they oppose. A second deadline of June 21, 1999 fared no better, the two main sticking points being EU customers' access to their data, and enforcement issues. The EU's new executive team had suggested a compromise under which American courts would enforce the "safe harbour" principles for aggrieved Europeans. A third deadline of October 1999 (the Directive's anniversary) was postponed to December 1999 in light of the negotiation's slight progress. No agreement was reached and yet another deadline was set--March 2000.

As we go to print, the two parties appear to have reached a tentative agreement; the EU will accept the "safe harbour" proposal but exclude financial services pending the coming into force of new American legislation on this sector. The agreement remains to be ratified by governments on both sides of the Atlantic and should come into force this summer. However, consumer and privacy advocates continue to disagree with the notion of "safe harbours", favouring the more prescriptive, restrictive and consumer-friendly Directive. EU officials have promised that they would cancel the agreement if Americans do not properly enforce it.

Other developments

A new data protection law came into force in **Austria** in January 2000. The new statute replaces the country's 1980 law and incorporates changes that reflect the more stringent requirements of the 1998 EU Directive. The **Czech Republic** has just passed a privacy protection bill making it illegal to collect personal data on people without their consent. The Senate is expected to approve the bill, which also creates a new Office for the Protection of Personal Data, somewhat akin to other national privacy or data protection commissions. **South Africa** has also just passed its *Promotion of Access to Information Bill*, which gives individuals access to government information (including their own data). This law is one of four statutes to implement the country's new *Bill of Rights* and to deal the final blow to the apartheid regime. **South Korea**'s new *Act on the Promotion and Protection of the Information Infrastructure* took effect on January 1st, 2000 and controls the collection, use and disclosure of personal information in telecommunications and electronic commerce.

The big picture

With passage of Bill C-6, Canada will join the swelling ranks of countries that protect their citizens' privacy in the public sector and, in most cases, the private sector as well. They do so in one of two ways.

First are those countries that recognise privacy —in some form— as a fundamental right either in their constitution or some other overarching law. This group includes Argentina, Belgium, Brazil, Bulgaria, Chile, the Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Iceland, Israel, Italy, Japan, South Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Peru, the Philippines, Poland, Portugal, Russia, the Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey and some states of the United States of America. In Canada, Québec is the only province to recognise the privacy of its citizen as a fundamental right in its *Civil Code*.

Secondly, there are those countries that have enacted specific data or privacy protection statutes (some which may already be listed above). This second group includes Australia (including some of its states like New South Wales), Austria, Belgium, Brazil, China's Special Administrative Region of Hong Kong, the Czech Republic, Denmark (including the self-governing Kalaalit Nunaat, formerly Greenland), Estonia, Finland, Germany (and all of its *Länder*), Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan (including some of its prefectures like Tokyo), South Korea, Lithuania, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Poland, Portugal, Russia, San Marino, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland (and all of its *Cantons*), Taiwan, Thailand, the United Kingdom (including the self-governing islands of

Guernsey, Jersey and Man) and the United States of America (including some states like Hawaii or New York). In Canada, all provinces (except Prince Edward Island) and territories have specific privacy legislation.

For more information on the above countries or on Bill C-6, please contact us or visit our Web site.

Stories we read in the news

GE Investments, the insurance and investments division of the General Electric Company, secretly recorded the identity of thousands of investors who responded to a 1998 mail survey of their personal financial information. The survey did not ask respondents to provide their name and address.

DoubleClick Inc., the Internet's largest advertising company, has put on hold its plan to link personal information to the anonymous data that it collects about consumers on the Internet.

A large working group of companies, ranging from Compaq and Oracle to Net Perceptions and Andromedia, is working on a new standard, Customer Profile Exchange, designed to integrate online and off-line customer data for use by companies wanting to gather information about consumers.

Online gift registries allow a business to collate information on both the buyer and the recipient.

A Parisian computer programmer is facing counterfeiting and fraud charges after developing a homemade "smart card" that he says gave him the ability to fraudulently purchase goods and services throughout France.

The U.S. Customs Service has been using the BodySearch device at several major airports to search for contraband. The machine uses low doses of X-rays to scan a traveller, displaying the outline of the person's naked body.

A new identity card access system at Ohio State University records the date and time of each transaction and the student's name in a database, whether the card is used for entering a residence hall or buying lunch.

RealNetworks stopped capturing and tracking data about the music files its customers downloaded from the Web—without telling consumers that they were being identified and monitored—following media attention and being served with a class action lawsuit over the privacy flaw. Even though TRUSTe (an online privacy seal of approval program) had certified the privacy statements on the company's site, it declined to take further action because the violation involved a piece of software, which falls outside TRUSTe's charter to police Web privacy practices.

A company called American Student Lists of New York obtains data on students from drivers licences, student directories, magazine subscriptions, yearbook publishers, school ring vendors, formal wear companies, fast food and book clubs. The trade in student data from this collection has led to several scholarship scams targeting immigrant, minority and rural students.

The security of Microsoft's free Hotmail email service—of which there are 2.5 million users in Canada—was compromised in August. The breach would have allowed an unauthorized user to read, delete and forward a Hotmail user's email by knowing only an easily guessed user name.

At a recent trade show, General Electric Co. demonstrated a concept for an Internet-connected refrigerator that is able to read bar codes as you put the groceries away and reorder by the time you need to shop. At the same trade show, Whirlpool Corp. showed a command-centre refrigerator, complete with food-tracking capability and a wireless pad to let consumers download recipes from the Net.

For the last four years, Mobiltrak of Birmingham, Alabama, has been marketing a device that finds out what radio stations people listen to in their cars. The company's clients pay to install the shoebox-size monitoring devices

at the entrances to their businesses, which work by picking up signals from a car radio's oscillator, the part of the radio that tunes in to the station. The data is recorded and sent to Moblitrak, which provides its clients with reports to help them determine whether the money they spend on radio advertising is being spent in the right places.

Maryland and Virginia will begin measuring highway congestion early next year by tracking motorists talking on cellular telephones as they drive the Capital Beltway. U.S. Wireless will install computer equipment on existing cellular towers to register the changing location of cell phone users and map the signals.

An Arkansas company, Acxiom Corp., that provides information to marketers has amassed 135 million consumer telephone numbers—including about 20 million that are unlisted—to help identify and profile people who call toll-free lines to shop or make an inquiry.

Police in Scotland are taking DNA from people stopped for any crime, even traffic offences. As well, the International Association of Police Chiefs has asked the U.S. Congress to require DNA samples from anyone arrested, and

New York City mayor Rudolph Giuliani has requested that the state legislature require DNA samples from every newborn baby. A Louisiana law that took effect on 1 September 1999 requires DNA to be taken from people arrested—but not necessarily convicted—of a violent crime.

In December, the U.S. Food and Drug Administration ordered Virginia Commonwealth University to suspend most of its medical research projects until it demonstrates that it has improved its procedures for protecting research subjects' privacy and safety.

A ground-breaking class action lawsuit against CVS Pharmacy Inc., and certain major pharmaceutical manufacturers was announced in November alleging that CVS used private customer information in its central database to target people for a direct mail marketing program that was funded and directed by the defendant pharmaceutical manufacturers.

A security breach at St. Joseph's Mercy Hospital in Pontiac, Michigan, left certain confidential patient records accessible to the public because the system did not require users to input a password or any other security roadblock. The hospital system uses an internal digital dictating service that allows doctors to record and access notes concerning recent patient examinations and consultations. The notes include information about patients, ranging from admitting and discharge data, to cardiac and mental health records.

Researchers at the University of California at Berkeley are building a minuscule robot in the size and shape of a fly for surveillance.

As part of a program of random drug testing on motorists this past August, police officers in Quebec pulled over randomly selected motorists at various checkpoints. Nursing students then asked the drivers whether they would care to volunteer a saliva or urine sample to detect drugs or— although not the study's prime focus—alcohol. If the motorists declined, they were free to drive away. If they complied, and test results later show them to be under the influence of drugs or alcohol, they faced no penalties.

Online marketing company Be Free has been granted a second patent covering certain methods of profiling consumer purchasing preferences, extending the coverage of the company's existing patent by including anonymous profiling.

Applied Digital Solutions, Inc. has acquired the patent rights to a technology that the company calls Digital Angel. Digital Angel is a transceiver that can be

implanted in the human body. The transceiver is powered electromechanically through the movement of muscles and can remain implanted and functional for years. It can be activated either by the "wearer" or by a remote monitoring facility. It can monitor certain biological functions of the human body—such as heart rate—and send a distress signal to a monitoring facility when it detects a medical emergency. The location of the device can be continuously tracked by Global Positioning Satellite technology.

A new security system being developed in Britain can identify individuals by the unique way in which they walk.

A new Levi's store in San Francisco is undertaking a large-scale voluntary collection of biometric marketing data by encouraging customers to give their fingerprints as well as personal data. Levi's enhances the customer's profile by adding his or her musical tastes. When the customer uses a CD listening station in the store, the system records which songs were switched off, and after how long. Customers can also use a private booth that scans their body in three dimensions to suggest an appropriate fit of jeans—called Levi's Original Spin. The dimensions are added to the customer's profile.

Corporate Management

The Privacy and Information Commissioners share premises and corporate services while operating independently under their separate statutory authorities. These shared services—finance, personnel, information technology and general administration—are centralized in Corporate Management Branch to avoid duplication of effort and to save money for both government and the programs. The Branch is a frugal operation with a staff of 15 (who perform many different tasks) and a budget representing 14 per cent of total program expenditures.

Resource Information

Managers continually pursue innovative approaches to deliver their programs without adversely affecting the quality level of service to the public. Treasury Board Ministers at their April 1998 meeting recommended an A-base review of the Offices' resource base, information technology needs and accommodation requirements. The Offices employed these additional resources to combat workload increases and carry-out their mandate while maintaining essential services.

The Offices' combined budget for the 1999-2000 fiscal year was $9,869,000. Actual expenditures for 1999-2000 were $9,760,574 of which personnel costs of $6,675,947 and professional and special services expenditures of $1,136,597 accounted for more that 80 per cent of all expenditures. The remaining $1,948,030 covered all other expenditures including postage, telecommunication, office and information technology equipment and office supplies.

Expenditure details are reflected in Figure 1 (resources by organization/activity) and Figure 2, (details by object of expenditure).

Figure 1: 1999-2000 Resources by Organization / Activity

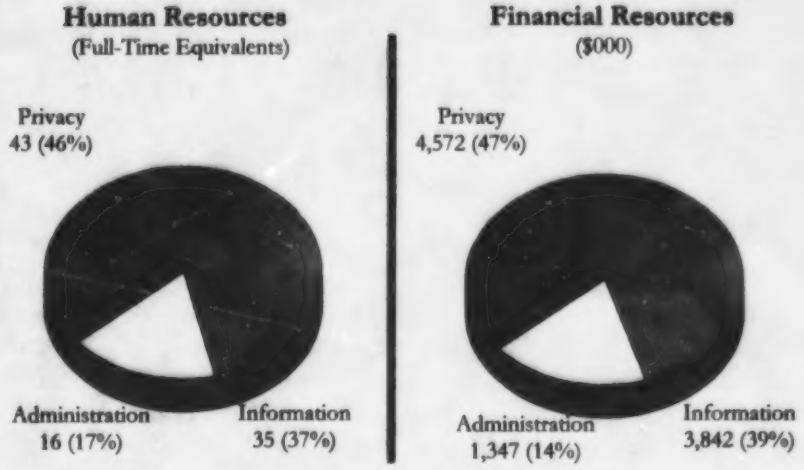


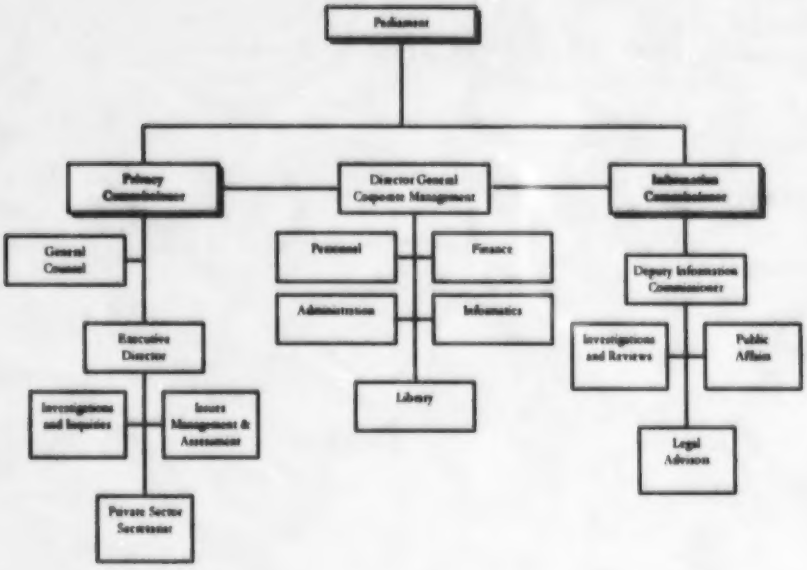
Figure 2: Details by Object of Expenditure

for the year ended March 31, 2000

	Information	Privacy	Corporate	Total
Salaries	2,200,135	2,750,322	751,490	5,701,947
Employee Benefit Plan Contrib.	388,000	453,000	133,000	974,000
Transport & Communication	84,030	106,430	105,952	296,412
Information	66,329	27,999	1,735	96,063
Professional & Special Services	383,442	574,001	179,154	1,136,597
Rentals	4,210	28,634	19,778	52,622
Purchased Repair & Maintenance	8,460	72,204	8,883	89,547
Utilities, Materials & Supplies	29,883	32,729	45,692	108,304
Machinery & Equipment	676,808	526,512	100,746	1,304,066
Other Payments	900	116	0	1,016
Total	**3,842,197**	**4,571,947**	**1,346,430**	**9,760,874**

* Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1999-2000 Public Accounts.

Organization Chart



A Tip of the Hat

My tenure as Privacy Commissioner, in addition to being an honour and privilege, has brought me a great many satisfactions. Not least has been the opportunity to work with a first-rate professional staff. I want to take this opportunity to thank all those who have showed so much dedication and enthusiasm over the last ten years. At the risk of inadvertently omitting someone (which would be truly an error, and no reflection on their work), they are:

* indicates members of staff as of March 31, 2000
** indicates members of staff out on secondment as of March 31, 2000

Ackroyd, Jeanette
Anderson, Colleen
Aubry, Benoit
Baggaley, Carman *
Baker, Barry
Barbaro, Tony *
Bastedo-Boileau, Catherine
Beaulé, Claude *
Bedley, Robert *
Bell, John
Bergeron, Michelle *
Blais, Anne *
Bloomfield, Stuart *
Boileau, Louise
Brault, Anne-Marie
Brault, Raymond
Brown, Grace *
Brunet, Josée
Carnegie, Doug **
Cliche, Nicole
Coolen, Gary *
Delisle, Julien *
Doré, Richard **
Doyle, Kathryn *
Dubuc, Philip
Dubuc, Thérèse *
Eadie, Kim
Evans, Jocelyne *
Fagan, Mike *
Fanjoy, Monique *
Farley, Francine
Fitzpatrick, Tom *
Fong, Marcus
Foran, Brian *
Gauthier, Yvon
Goldsmith, Ann *
Gow, Glenn
Gravelle, Robert
Hamilton, Joanne *
Harris, Holly *
Hébert, Raymond *
Henry, Gary

Imbeault, Marie-Andrée *
Jackson, Sally
Khosla, Jay *
Kirkby, Hedy
Labelle, Louise *
Lacroix, Ginette
Lafleur, Ann-Marie *
Lapierre, Don
Lavoie, Chantal *
Lavoie, Roxanne
Leblanc-McCulloch, Monique *
Lévis, Jacques *
Lystiuk, Fred *
Mann, Don
Martelock, Cathy *
Maurel, Richard-Philippe *
Maynard, Peter
McAuliffe, Ann
McLean, Joyce *
Ménard, Nicole *
Millar, Melanie *
Montigny, Gerry
Mullen, Dennis
Nantel, Martine *
Neary, Gerald *
Netterfield, Carolyn
Oscapella, Eugene
Pavlis-Gougeon, Virginia *
Perreault, Renée
Peszat, Jan *
Richard, Paul *
Richer, Michel
Rodrigue, Jocelyne *
Rooke, Anne *
Roy, Rachelle
Roy, Jocelyn
Savas, Eric
Schwartz, Virginia *
Scott, Pat
Sérafin, Nicole *
Sicotte, Nicole *
St-Pierre, Chantal *
Stewart, Brian *
Tessier, Isabelle
Thériault, Natalie *
Thibaudeau, Monique *
Trottier, Ghislaine
Van Berkel, Gerry
Welke, Ron
Wheeler, Susan *
Wolchuk, Ron

Commissaire
à la protection de la vie privée

RAPPORT ANNUEL
1999-2000

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 1999
N° de cat. IP 30-1/2000
ISBN 0-662-64957-5

Cette publication est offerte sur cassette et sur disquette informatique.
Nous sommes accessibles sur le réseau Internet à l'adresse : http://www.privcom.gc.ca

Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

mai 2000

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1er avril 1999 au 31 mars 2000.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips

Bruce Phillips

Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

mai 2000

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1er avril 1999 au 31 mars 2000.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips

Bruce Phillips

Remerciements

Nous remercions les caricaturistes dont les œuvres égaient le présent rapport annuel : John Grimes, Cathy Guisewite et Chris Slane. Nous remercions également Peter Lefebvre de CURSOR Communications, créateur de notre page couverture, et Guylaine Duval du Groupe Communications Canada, responsable de l'impression de ce document.

Un bref temps d'arrêt…avant de continuer de plus belle

La promotion et la défense de la vie privée nous procurent beaucoup de plaisir, ce qui ne nous empêche pas dans les moments plus difficiles de nous interroger sur le pourquoi de nos efforts. Chacun d'entre nous a sa vision de ce que représente la vie privée, et les citations qui suivent nous rappellent son importance.

Qu'est-ce que la vie privée ?

…le droit de vivre en paix — le plus complet de tous les droits et celui le plus prisé des civilisations.

— Louis Brandeis, juge associé de la Cour suprême des États-Unis d'Amérique, 1928

Cache ta vie

— attribué à Néoclès, père d'Épicure, 3ième siècle avant JC

Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend.

— tiré du rapport L'ordinateur et la vie privée, 1972

Savoir dissimuler est le savoir des rois.

— Louis Armand du Plessis de Richelieu, homme politique français, 1640

La civilisation est le progrès d'une société vers la vie privée. L'existence du sauvage est publique et réglée par les lois de sa tribu. La civilisation est le processus de libération par l'homme de l'homme.

— Ann Rand, auteure, 1943

Mon âme a son secret, ma vie a son mystère.

— Félix Arvers, poète, 1833

Un homme a le droit de choisir de vivre sa vie sans que sa photo soit publiée, ses affaires commentées, ses succès répertoriés pour le bénéfice d'autrui ou ses excentricités commentées, et ce que ce soit par des placards, des circulaires, des catalogues, des journaux ou des périodiques.

— Alton B. Parker, juge en chef de la Cour d'appel de l'État de New York, 1901

La parfaite valeur est de faire sans témoins ce qu'on serait capable de faire en public.

— François de la Rochefoucauld, moraliste, 1664

Si une société sans justice sociale n'est pas une bonne société, alors une société sans vie privée est nécessairement une société sans justice sociale. Nous devons fonctionner en sachant que l'individualité est une chose sacrée à préserver comme si nos vies en dépendaient — parce que c'est le cas.

— Auteur inconnu

Il est reconnu depuis longtemps que la liberté de ne pas être obligé de partager nos confidences avec autrui est la marque certaine d'une société libre.

— Gérard La Forest, juge de la Cour suprême du Canada, *R. c. Duarte*, 1990

Le droit à la vie privée est le droit d'un individu, d'un groupe ou d'une entreprise de déterminer quand, comment et jusqu'à quel point ses renseignements seront communiqués à d'autres.

— Allan Westin, professeur, 1967

La notion de vie privée se rapporte entièrement au respect que nous avons de l'unicité d'autrui. Chaque individu a ses propres valeurs, qu'il choisit ou non de révéler. Le respect de cet individu exige que nous lui laissions vivre une vie privée. Le respect de cette vie privée favorise la liberté, l'autonomie et la dignité. L'alternative est une vie vide de sens et pleine de crainte, soumise à l'oppression d'une perpétuelle surveillance.

— Bruce Phillips, Commissaire à la protection de la vie privée du Canada, 1999

Table des matières

Réflexion personnelle **1**
Ces dix dernières années **3**
La loi C-6 : de l'ordre dans le secteur privé **27**
Perceptions canadiennes sur la vie privée : confiance et contrôle .. **34**
Renseignements médicaux : trop publics ! **38**
Progrès de l'inforoute canadienne de la santé, et protection des patients 43
La loi albertaine sur les renseignements en matière de santé — Qu'en est-il au juste ? 47
Un numéro permanent d'identification pour les médecins 49
Réforme de la *Loi sur la protection des renseignements personnels* **50**
L'avenir du recensement **57**
Le recensement de 2001 — une collecte plus claire 57
Données de recensements antérieurs 61
Le point sur le numéro d'assurance sociale **65**
Le dossier unique sur chaque citoyen existe... à DRHC **73**
Sur la colline **80**
Le point sur la *Loi sur le recyclage des produits de la criminalité* 86
Dédouanement et vie privée des passagers 89
Renseignements sur les contribuables, ou statistiques ? 91
Combler les lacunes : Une charte des droits relatifs à la vie privée 94
Direction de l'Analyse et de la gestion des enjeux **96**
Les études d'impact sur la vie privée 96
Partage des données à l'Agence des douanes et du revenu du Canada (ADRC) 99
Sondages de la clientèle 100
Centre et Registre canadiens des armes à feu — Ministère de la Justice du Canada 104
Couplages avec les dossiers de Prestation fiscale pour enfants 104
Disparition d'un ordinateur portatif à Halifax — Service correctionnel du Canada 106
Communication dans l'intérêt public — Renseignements médicaux d'un membre décédé des Forces canadiennes 108
Un respect trop littéral de la Loi : rapports annuels des institutions fédérales 108

Table des matières (suite)

Direction des enquêtes et demandes de renseignements **111**
Définitions des conclusions possibles de nos enquêtes 114
L'art de lire à l'envers 117
Un consentement bien peu éclairé 119
Vous pourriez être quelqu'un d'autre ! 121
Abus de pouvoir 124
Un justicier controversé 126
Un colis bien dur à retrouver 127
Mais qui est responsable, au juste ? 129
Des conducteurs manitobains jetés aux ordures 131
Une négligence qui aurait pu être dangereuse 133
Protégeons nos renseignements à l'extérieur du bureau 136
Destruction illégale et intentionnelle de documents 137
Rien ne vaut une explication claire 139
Question de patience... 141
Neuf moins trois font plus...pour notre vie privée ! 142
Demandes de renseignements 145
Devant les tribunaux **154**
Leçons des dix dernières années 154
Dossiers actifs 156
Coup de pouce à la Loi C-6 ..... **159**
La technologie à l'aide de notre vie privée sur l'Internet 159
L'Association canadienne du marketing veut protéger les enfants ... 162
Mise à jour sur la protection de la vie privée **164**
La vie privée dans les provinces et les territoires 164
La vie privée de par le monde 167
Ce que nous apprennent les journaux **172**
Gestion intégrée **178**
Personnel du Commissariat **181**

Réflexion personnelle

Voilà bientôt 10 ans que j'occupe mon poste. Ce rapport annuel se veut donc une sorte de rétrospective résumant les faits saillants de cette dernière décennie.

Nombreux sont les progrès, grands ou petits, dont parle ce rapport et qui découlent des activités de mon Commissariat. Mais il nous en reste encore beaucoup à accomplir dans cette lutte que nous menons pour le droit de vivre libre de toute surveillance et de toute atteinte à notre vie privée.

L'adoption toute récente d'une loi protégeant cette vie privée dans le cadre de nos transactions avec le secteur privé est la plus importante nouveauté de ces dix dernières années. Cette loi s'appliquera à une majorité des renseignements transigés dans le secteur privé. Mais elle ne répond pas à toutes les attentes, car il nous manque encore une protection juridique contre, entre autres, la surveillance vidéo, le prélèvement abusif de substances corporelles, l'abus de nos renseignements médicaux et génétiques et l'exagération en matière de dépistage génétique et antidrogue.

Il faut aussi réviser la législation régissant la gestion des fonds de renseignements personnels du gouvernement fédéral. En effet, la *Loi sur la protection des renseignements personnels* a presque 20 ans, et impose à certains chapitres des obligations moindres que celles énoncées dans la nouvelle loi visant le secteur privé. Ce devrait être l'inverse, et il faut s'attaquer à ce problème au plus tôt.

Nul n'ignore désormais le fait que les dix dernières années ont vu une révolution dans la gestion de l'information, causée par les phénoménales avancées en informatique et en télécommunications. Pourtant, nos lois sont encore loin de nous permettre de dominer cette technologie — au lieu de l'inverse actuel — et de nous libérer en tant que race humaine.

Quant à moi, je considère que ces 10 ans m'ont procuré le plus grand honneur et privilège de ma vie, soit celui de me porter à la défense de mes concitoyens. Mon rôle d'officier parlementaire en est un que Teddy Roosevelt n'aurait pas décrié : s'y consacrer au seul nom de l'avancement de la liberté humaine, et ce sans peur ni favoritisme, voilà de quoi rendre ce rôle puissant.

Je ne peux cependant pas dissimuler une certaine tristesse : toutes les personnes que j'ai rencontrées ces dix dernières années appuyaient haut et

fort le droit à la vie privée ; et pourtant, certains de leurs gestes détruisaient ce même droit ! Il ne suffit pas de dire quelque chose, il faut aussi le vivre. Mon poste exige donc un certain scepticisme, mais aussi de l'optimisme.

Je conclus ici en attribuant une bonne partie des succès de mon Commissariat à mes employé(e)s hors pair, convaincu(e)s et dévoué(e)s. Leurs noms apparaissent à la fin de ce rapport, et je leur dois beaucoup.

Le Commissaire à la protection de
la vie privée du Canada

Bruce Phillips

Ces dix dernières années

Rationalisation et privatisation du gouvernement
Au cours de la dernière décennie, tous les échelons de gouvernement ont dû faire face à des pressions implacables pour éliminer le gaspillage et pour administrer et offrir des produits et des services publics de façon plus efficiente. Les gouvernements ont réagi en confiant certaines de leurs fonctions à des non-fonctionnaires — l'impartition — et certaines de leurs activités au secteur privé, en centralisant et en consolidant leurs opérations, et en concluant des ententes de partenariat sur la prestation de services avec d'autres paliers de gouvernement.

Clauses de contrat sur la protection des renseignements personnels
Ces tendances, qui contribuent peut-être à une administration publique plus efficiente, ont également miné et permis de contourner la loi qui protège les droits des Canadiens à la protection de leurs renseignements personnels. L'impartition a été la première de ces tendances. Elle nous a amené à tenter d'endiguer le flot des renseignements personnels confiés au secteur privé sans protection adéquate au chapitre de la vie privée.

Nous avons toujours allégué que les sous-traitants embauchés par le gouvernement deviennent des « agents » de la Couronne et sont donc assujettis à la *Loi sur la protection des renseignements personnels*. Cependant, bien des sous-traitants n'ont ni reconnu ni respecté ce principe et ont traité les renseignements qu'ils ont recueillis ou produits comme s'ils étaient les leurs. Pour mettre fin à ce moyen de contourner la Loi, nous avons commencé à travailler avec l'ancien ministère d'Approvisionnements et Services Canada et le Conseil du Trésor pour élaborer les modèles de contrat de services assortis de clauses conçues spécialement pour que le sous-traitant soit tenu de respecter la Loi. Toutefois, des années plus tard, nos vérifications continuent de mettre au jour des contrats qui ne sont pas assortis de telles dispositions.

Privatisation
L'impartition présentait un défi gérable ; la privatisation de pans complets du gouvernement était une autre paire de manches. Les menaces posées à la vie privée par la privatisation ont été révélées au grand jour en 1995, année où l'on a privatisé le système canadien de contrôle de la circulation aérienne. La création de NAV Canada a enlevé à quelque 6 000 fonctionnaires fédéraux et aux dossiers personnels de milliers d'autres utilisateurs du système la protection que leur accordait auparavant la *Loi sur la protection des renseignements personnels*. Ces utilisateurs n'avaient désormais plus le droit d'accéder à leurs renseignements personnels ni de les contrôler. Le gouvernement a ignoré nos

recommandations répétées d'assujettir la nouvelle entité à la *Loi sur la protection des renseignements personnels*, ce qui, selon nous, constituait rien de moins qu'un désastre sur le plan de la protection de la vie privée. Mais une leçon a peut-être été tirée, puisque la privatisation de l'Administration de la voie maritime du Saint-Laurent s'est effectuée selon les règles.

Lorsque le gouvernement fédéral ne se débarrassait pas de biens importants, il fusionnait, centralisait et consolidait ses activités en de nouveaux ministères ou des ministères restructurés. Le meilleur exemple en reste l'amalgame, en 1994, de diverses composantes des ministères de l'Emploi et de l'Immigration, de la Santé et du Bien-être social, du Travail, du Multiculturalisme et de la Citoyenneté, et du Secrétariat d'État pour former Développement des ressources humaines Canada (DRHC). Ce nouveau « super ministère » s'occupe de domaines aussi vastes que l'assurance emploi, les pensions, la santé et la sécurité au travail, les prestations d'aide aux enfants et aux familles, les prestations d'invalidité, l'éducation, la formation professionnelle et la création d'emplois. Du fait de la fusion, un seul et même ministère est responsable d'une quantité et d'un détail de renseignements personnels sans précédent dans l'histoire du Canada. DRHC s'infiltre dans presque tous les aspects de la vie des Canadiens.

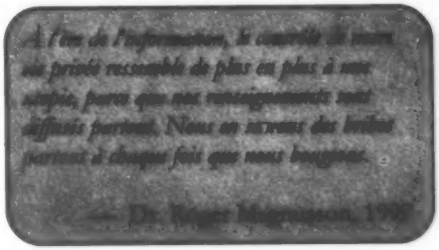
Technologie de la gestion de l'information

L'explosion de la technologie de l'information dans les années 90 a donné au gouvernement un nouvel outil pour réduire les coûts et améliorer l'efficience administrative. En 1994, dans le cadre de son *Plan directeur pour le renouvellement des services gouvernementaux à l'aide des technologies de l'information*, le gouvernement a présenté son plan, qui consistait à utiliser les technologies informatiques de pointe pour « rationaliser », « restructurer » et « moderniser » la fonction publique fédérale. Le rapport mettait de l'avant la proposition de créer une toile électronique intégrée qui relierait tous les secteurs du gouvernement grâce à un système de communications normalisé et compatible qui permettrait aux gouvernements fédéral et provinciaux, ainsi qu'aux entreprises privées qui fournissent des services gouvernementaux, de partager de l'information.

En prévision des répercussions de cette technologie sur la vie privée des citoyens, nous avons dressé une « liste de contrôle de la vie privée », que nous avons publiée dans le rapport annuel de 1992-1993. Son but était d'informer les hauts fonctionnaires du gouvernement des répercussions que pourraient avoir les nouveaux systèmes de gestion de l'information sur la vie privée, et pour aider les ministères à concevoir et à mettre en application ces nouveaux systèmes en tenant compte de la vie privée. Même si le Plan directeur reconnaissait la nécessité d'assurer « la sécurité, l'intégralité et la

confidentialité » de l'information, à bien des égards, les recommandations formulées dans le rapport venaient directement contredire les principes de la vie privée. Comment, par exemple, le fait d'échanger les renseignements avec divers ordres de gouvernements et avec le secteur privé peut-il être compatible avec le principe fondamental de la vie privée selon lequel le gouvernement ne devrait utiliser ou communiquer des renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis ? Nous avons averti les gens que certains éléments du Plan directeur pourraient démanteler les protections assurées aux données personnelles par la *Loi sur la protection des renseignements personnels* fédérale.

Une autre technologie de pointe du traitement des données, l'« entrepôt de données », est apparue dans les années 90. DRHC a été l'un des premiers ministères fédéraux à reconnaître son potentiel en tant qu'outil de gestion de l'information et à installer ce genre de système. Un entrepôt de données intègre des données provenant de diverses sources et de divers endroits dans un dépôt électronique central où l'information est normalisée et mise à la disposition d'un certain nombre d'utilisateurs afin qu'ils puissent s'en servir et les manipuler. Pour les gestionnaires, ce système présente un potentiel stimulant. Pour ce qui est de la vie privée, cependant, ces entrepôts sont dangereux, car des renseignements personnels recueillis à une fin donnée pourraient être utilisés à des fins différentes sans rapport avec les fins initiales. Ces entrepôts permettent également de dresser un portrait assez précis de chaque client, comportant même des caractéristiques jusqu'alors inconnues et découvertes grâce à d'anciennes transactions ou relations.



Numéros personnels d'identification

Un numéro unique d'identification permettant de relier une personne à ses renseignements est essentiel tant à la vision qu'a le Plan directeur d'une fonction publique « intégrée horizontalement » qu'aux initiatives comme l'entreposage de données. Comme le système regroupe de si nombreux partenaires, chacun veut s'assurer que la personne dont il recueille les renseignements et à qui il offre des services est la bonne. Pas surprenant, donc, que le processus global de « restructuration » du gouvernement exige un numéro national d'identification de la clientèle. Pas surprenant non plus que ce numéro semble devoir être le numéro d'assurance sociale (NAS), qui

joue déjà pratiquement ce rôle du fait de l'absence de contrôles législatifs sur son utilisation.

Au milieu des années 90, un groupe de gestionnaires de la technologie de l'information des ministères de la sécurité du revenu des gouvernements fédéral, provinciaux et territoriaux ont commencé à étudier la faisabilité d'un numéro national d'identification de la clientèle. Dans un rapport de 1996, le groupe concluait que l'utilisation d'un tel numéro (et de sa base de données connexe) profiterait grandement aux gouvernements. Parmi les avantages possibles, mentionnons l'identification des prestataires admissibles avant le versement des prestations, l'élimination des coûts dédoublés associés à l'émission de multiples numéros d'identification et la facilitation des couplages exacts de données pour détecter la fraude. Même si le groupe avait envisagé plusieurs options, il concluait que la meilleure consistait à « moderniser » le NAS. Il recommandait aussi d'assortir la carte d'assurance sociale de dispositifs de sécurité améliorés — notamment une composante biométrique visant à prévenir la contrefaçon et à prouver avec précision que la carte appartient à son détenteur. Nous n'étions d'accord qu'avec un seul aspect du rapport : sa conclusion voulant que la vie privée soit le seul obstacle important à l'élaboration d'un numéro national d'identification de la clientèle.

Le rapport que le Vérificateur général a déposé en 1998, intitulé *La gestion du numéro d'assurance sociale*, confirmait les doutes de longue date selon lesquels le cadre législatif et administratif qui régit actuellement le NAS ne sert ni les intérêts du gouvernement ni les droits du public à sa vie privée. Non seulement le Vérificateur général a recommandé d'apporter des améliorations à l'administration du NAS, mais il a aussi exhorté le Parlement à examiner les enjeux stratégiques plus vastes associés au numéro, particulièrement son rôle possible de numéro national d'identification de la clientèle. Le Parlement a réagi à sa demande en mandatant le Comité permanent de la Chambre des communes sur les droits de la personne et la condition des personnes handicapées pour étudier l'administration et le régime des politiques régissant le NAS. Le Comité permanent a déposé son rapport intitulé *Au-delà des chiffres : L'avenir du numéro d'assurance sociale au Canada* au printemps 1999 et commandé à DRHC de préparer d'ici la fin de la même année un rapport qui établirait le rôle futur du NAS en tant que numéro national d'identification.

Les préoccupations relatives à la vie privée sont au cœur des débats entourant le NAS depuis sa création. L'opposition publique à l'idée que le NAS devienne un numéro universel d'identification, renforcée par les recommandations formulées dans *Une question à deux volets*, fruit de l'examen d'un comité parlementaire, a amené le Conseil du Trésor à élaborer en 1989

une directive limitant la façon dont le gouvernement fédéral peut utiliser le NAS. Tous les commissaires à la vie privée ont signalé les dangers liés à l'établissement d'un système universel d'identification, qu'il s'agisse d'un NAS modifié ou d'un autre numéro. Nous avons répété ces avertissements, mais peut-être jamais avec autant de vigueur que nous ne l'avons fait à la fin des années 90, lorsque le gouvernement s'est très sérieusement penché sur la possibilité d'adopter un système universel d'identification de sa clientèle.

Notre appréhension tient au fait que nous pourrions perdre le contrôle : contrôle des renseignements que d'autres personnes ont sur nous, contrôle de la façon dont ils utilisent ces renseignements, contrôle de notre capacité d'influer sur les événements et les décisions qui touchent notre vie, et enfin contrôle de notre capacité de faire des choix en fonction de nos intérêts personnels rationnels. Un système universel d'identification menace de miner notre contrôle en permettant à n'importe quel organisme d'utiliser le numéro pour obtenir de l'information sur nous à notre insu ou sans notre consentement. Il augmente de beaucoup la capacité des gouvernements de recueillir des renseignements auprès de diverses sources et de dresser notre portrait, ainsi que de surveiller et de suivre nos faits et gestes. Si le numéro est obligatoire — ce qui est presque inévitable lorsqu'il est utilisé par un grand nombre de personnes et qu'il est requis par tous les ministères et organismes gouvernementaux — il devient un « passeport interne » sans lequel nous n'existons pas. Dans l'infrastructure publique « intégrée horizontalement » envisagée dans le Plan directeur du gouvernement fédéral, un numéro national d'identification de la clientèle menace notre autonomie personnelle en soumettant notre vie à un examen minutieux continuel.

En décembre 1999, DRHC a déposé son exposé de principes sur le NAS. À notre grand soulagement, l'exposé rejetait l'idée de transformer le NAS en numéro national d'identification. DRHC donnait deux raisons à ce rejet : les coûts prohibitifs et la faible rentabilité d'un tel scénario, et les graves problèmes qu'il entraînerait pour la vie privée. Cependant, l'exposé de principes, discuté plus loin dans le présent rapport, a ignoré la recommandation du Comité permanent (et la nôtre) d'imposer des restrictions législatives à l'usage du NAS, et n'a pas rejeté l'idée d'utiliser le numéro comme numéro national d'identification de la clientèle. Nous n'avons donc pas avancé.

Réseaux électroniques et l'Internet

Le fait que le gouvernement ait remplacé graduellement la gestion et les communications de ses dossiers papier par des systèmes électroniques a provoqué des préoccupations grandissantes quant à l'intégrité et à la sécurité des données. Contrairement au courrier conventionnel, l'information

transmise par voie électronique n'offre pas d'enveloppe cachetée pour protéger la confidentialité ni de systèmes éprouvés pour assurer une livraison sécuritaire. Ni l'expéditeur ni le destinataire ne peuvent contrôler (ou savoir) qui lit son courriel pendant qu'il est acheminé. Les individus dont les renseignements personnels sont échangés par l'entremise de systèmes ouverts risquent de voir leur vie privée compromise : de tels systèmes permettent à n'importe quel usager autorisé de lire, de copier, de surveiller, de modifier ou même de détruire le message acheminé. Et les employés ne sont pas en reste, qui peuvent devenir assujettis à une surveillance électronique constante.

Le Secrétariat du Conseil du Trésor a toutefois reconnu les répercussions qu'ont eues ces nouvelles pratiques sur les employés et a élaboré une politique sur l'utilisation des réseaux électroniques, publiée en 1998. La politique précise les attentes et les droits des employeurs et des employés qui utilisent des réseaux électroniques au travail. La politique reconnaît que les employés ont des attentes raisonnables en matière de protection de leur vie privée au travail, même s'ils utilisent le matériel du gouvernement. La politique définit et limite également les cas où les hauts fonctionnaires peuvent surveiller ou intercepter de façon licite les communications transmises sur le réseau gouvernemental : s'il existe des motifs raisonnables de croire qu'un employé utilise le réseau à mauvais escient ou lorsque la surveillance fait partie d'un programme d'entretien de routine du réseau. Même si la politique reconnaît les attentes des employés en termes de leur vie privée au travail, elle suggère qu'un employeur peut réduire ces attentes en se bornant à aviser les employés qu'il y aura surveillance.

Évidemment, lorsque les réseaux électroniques permettent de traiter avec le gouvernement, ils menacent la vie privée du public. Au milieu des années 90, le gouvernement fédéral a commandé des sondages pour évaluer l'aise de la population face aux nouvelles technologies interactives et son intérêt à y recourir pour ses transactions avec le gouvernement. Les enquêtes ont toutes révélé l'extrême préoccupation du public face à la sécurité des transmissions électroniques ainsi que la capacité des systèmes de protéger la vie privée. Ces résultats ont mené le Conseil consultatif national de l'autoroute de l'information, qui élaborait la stratégie du gouvernement fédéral relative à l'autoroute de l'information du Canada, à une conclusion inévitable : pour que le gouvernement réussisse à moderniser sa fonction publique et à préparer l'économie canadienne à l'ère de l'information, il lui fallait absolument rassurer le public que les transactions électroniques sont à l'épreuve d'accès, de surveillance, de changements et d'abus non autorisés.

Vers la fin des années 90, le cryptage était perçu comme un outil important de protection des transmissions électroniques. Le cryptage est la science de la

transformation d'un texte clair en texte chiffré et inversement. Il est soutenu par une Infrastructure à clé publique (ICP). La cryptographie ICP est fondée sur un système à deux clés : une clé publique (connue d'un grand nombre de personnes) qui permet de coder les données, et une clé privée (connue d'une seule personne) qui permet de décoder les données. Même si les deux clés sont complémentaires, il est impossible de dériver la clé privée de la clé publique. Ainsi, seule la personne qui détient la clé privée peut décoder le message. Ce système, couplé à un système d'authentification numérique, est prometteur pour la protection de la confidentialité des communications électroniques et de la vie privée de ses utilisateurs.

Le système du gouvernement fédéral exige toutefois qu'une autorité de confiance génère les clés, certifie leur validité et gère leur distribution sécuritaire. C'est là le talon d'Achille de ce système : pour qu'il soit utilisable, il faut qu'une autorité centrale connaisse la clé privée de chacun et soit donc investie du pouvoir de décoder toutes nos communications. La Société canadienne des postes et le Centre de la sécurité des télécommunications ont tous deux été pressentis comme autorité de confiance. Entre-temps, plusieurs ministères fédéraux (Santé Canada, Développement des ressources humaines Canada et Travaux publics et Services gouvernementaux Canada) mettent à l'essai la technologie ICP. Les résultats permettront de déterminer son application plus universelle. Toutefois, le Canada devra débattre vigoureusement du sujet avant d'ouvrir la porte à nos communications les plus personnelles à quelque organisme que ce soit.

Surveillance en milieu de travail et des lieux publics

En 1992, dans le cadre d'une présentation à des professionnels des ressources humaines, un haut gestionnaire du Commissariat à la protection de la vie privée proposait l'inclusion du concept de vie privée dans l'approche éthique globale des relations de travail. Il faisait particulièrement référence aux menaces « traditionnelles » à la vie privée en milieu de travail : collecte excessive de renseignements personnels d'employés, mauvaise utilisation des renseignements, refus ou accès limité à ceux-ci, et communications négligentes à des personnes ou organismes externes. Mais notre gestionnaire mentionnait aussi en passant le dépistage antidrogue, le dépistage génétique et la surveillance électronique, cette dernière menace commençant à peine à apparaître, résultant de l'informatisation et de la gestion électronique de l'information.

Historiquement, la surveillance systématique en milieu de travail remonte à Frederick Taylor et son système de mesures détaillées et précises des gestes de chaque ouvrier. L'effacement graduel de la ligne de démarcation entre les intérêts légitimes des employeurs et les droits à la vie privée des employés

remonte également à très loin dans le temps. Henry Ford, qui envoyait des inspecteurs de sa « division sociologique » dans les maisons de ses ouvriers pour vérifier leur moralité, n'était ni le premier ni le dernier patron à vouloir se pencher sur plus que les résultats au travail de ses employés.

Les temps modernes ont déjà dépassé les fouilles, les vérifications d'antécédents, les détectives privés, le dépistage médical et psychologique et les détecteurs de mensonge. Désormais, nous avons affaire à des systèmes de télévision en circuit fermé, la surveillance de tout ce que nous tapons à notre ordinateur, la surveillance informatisée de notre utilisation d'un véhicule, le pistage constant de nos moindres déplacements en milieu de travail, et la surveillance de nos appels téléphoniques, du temps que nous passons sur l'Internet, et des messages électroniques que nous envoyons.

Les employeurs ont certes raison de se préoccuper de sécurité, d'espionnage commercial, de leur réputation, du milieu de travail et des risques possibles de surcharge et de pannes de leurs systèmes informatiques. Mais vigilance ne devrait pas rimer avec hystérie : les systèmes de surveillance mis en place peuvent avoir des conséquences beaucoup plus lourdes que les problèmes qu'ils souhaitaient au départ régler.

L'abus des systèmes de surveillance est un risque évident : la valeur d'un système est proportionnelle à celle des personnes qui l'opèrent. La surveillance qu'exerce un employeur peut outrepasser ce qui est de son ressort et porter sur des activités syndicales ou l'identification de dénonciateurs. Un désir de nuire peut pousser quelqu'un à monter un dossier négatif sur certains employés. Des renseignements de nature délicate peuvent tomber en de mauvaises mains et être utilisés à des fins de chantage.

Même l'utilisation conforme de systèmes de surveillance soulève des questions préoccupantes. Étant donné la longueur de la journée de travail, peut-on en toute raison totalement interdire aux employés de communiquer librement et sans surveillance avec leur famille, leurs amis ou d'autres ? Les célibataires qui travaillent à temps plein n'ont quelquefois pas d'autre choix que de s'occuper de choses

personnelles à partir de leur lieu de travail. En outre, la communication au travail est inévitable. De telles interactions peuvent permettre d'endurer le travail le plus ennuyeux, et même de générer de nouvelles idées quant à la façon d'améliorer le rendement. Il est également raisonnable de croire que les gens ont besoin de se détendre au cours de leur journée de travail.

Bref, nous avançons que les employés sont en droit de s'attendre à une qualité de vie raisonnable en milieu de travail, dont la vie privée est une composante essentielle. Ce besoin est encore plus grand avec l'augmentation du nombre de télé-travailleurs et la disparition graduelle de la frontière entre la maison et le bureau — sans oublier la nécessité de limiter ces prétendus liens entre nos activités personnelles en dehors des heures ouvrables et notre rendement professionnel.

Le double rôle du Commissariat, soient la surveillance de l'application de la *Loi sur la protection des renseignements personnels* par les institutions fédérales et le suivi des questions émergentes de vie privée débordant du cadre de cette Loi nous permet un point de vue intéressant. Nous soulignons avec plaisir le fait que les institutions fédérales ont su jusqu'à présent éviter les excès notés chez d'autres employeurs.

Dans notre rapport annuel de 1992-1993, nous relevions le fait que le ministère des Communications entendait développer une carte à puce pour ses employées, laquelle servirait de porte-monnaie électronique, contrôlerait l'accès aux divers systèmes informatiques, contribuerait à l'inventaire de l'équipement de haute technologie et contrôlerait les entrées et sorties des employés. Nous écrivions que l'application la plus répandue pour une carte capable de valider l'identité, la situation d'emploi ainsi que la cote sécuritaire de quelqu'un serait d'en faire une carte de fonctionnaire, laquelle pourrait cependant devenir un outil de surveillance. Le gouvernement devrait donc établir des normes et lignes directrices en régissant l'utilisation.

Dans le même rapport, nous parlions du Comité fédéral du projet de télétravail, chargé d'évaluer un projet pilote de trois ans permettant aux employés de travailler à la maison et d'expédier leur travail électroniquement. Un tel projet visait de bons objectifs : un meilleur équilibre des exigences professionnelles et de la vie personnelle des employés, et une réduction de la consommation d'énergie, de la pollution et de la congestion routière. Mais nous nous préoccupions de l'existence de mécanismes protégeant notre vie privée, la confidentialité des renseignements personnels apportés à la maison et transmis électroniquement et la qualité de vie personnelle des télé-travailleurs, sans compter des risques inhérents à la surveillance et au suivi de ces derniers.

En 1994 nous rapportions que la Monnaie royale canadienne surveillait les conversations téléphoniques de ses employés. Malgré ses réserves, le Commissaire a conclu que cette pratique n'allait pas à l'encontre de la *Loi sur la protection des renseignements personnels* puisque la surveillance était effectuée à des fins d'évaluation du rendement et que les employés étaient avertis à l'avance. Le Commissaire a cependant rappelé aux gestionnaires de la Monnaie le droit de leurs employés de prendre connaissance de toute note prise pendant la surveillance, et a recommandé à l'organisme d'adopter des marches à suivre respectant la vie privée des personnes impliquées, dont le public contactant la Monnaie. Les gestionnaires de ce dernier organisme ont alors entrepris de donner suite à nos recommandations.

La surveillance vidéo était le sujet d'une plainte discutée dans le rapport annuel de 1997-1998. Nous y soulignions que l'utilisation de caméras vidéo cachées, de par sa nature très envahissante, exige une justification à toute épreuve. Inquiet des impacts sur la vie privée, le Commissaire a écrit au Conseil du Trésor pour l'inciter à développer une politique gouvernementale sur le recours à de telles caméras. Il recommandait que la politique spécifie clairement que la surveillance doit reposer sur des soupçons raisonnables et n'être effectuée qu'en dernier ressort, qu'elle respecte les attentes raisonnables des gens face à leur vie privée, et qu'elle se limite le plus strictement possible à la personne soupçonnée. Quoique se rapportant particulièrement à la surveillance vidéo, ces recommandations s'appliquent fort probablement à toute forme de surveillance en milieu de travail.

Certaines des préoccupations du Commissaire ont été relevées par le Conseil du Trésor dans sa politique publiée en 1998 sur l'utilisation des réseaux électroniques. Bien qu'incomplète, tel qu'expliqué précédemment, cette politique a fait en sorte que les réseaux électroniques ne deviennent pas une « prison électronique ». Puis en avril 1999, le Conseil du Trésor a publié une politique sur la surveillance vidéo qui adoptait toutes les recommandations faites par le Commissaire l'année précédente.

Les bureaux fédéraux ne sont donc pas devenus les univers orwelliens que certains craignaient. Cela est attribuable en grande partie à la reconnaissance bien établie des principes de pratiques équitables de gestion de l'information enchâssés dans la *Loi sur la protection des renseignements personnels*, et au fait que les questions de vie privée sont débattues et discutées dans un contexte juridique. Le Commissariat pourrait même se féliciter quelque peu.

Restant sur le sujet de la surveillance du courriel et de l'accès des fonctionnaires à l'Internet, un gestionnaire aurait récemment déclaré : « Votre pays est peut-être une démocratie, mais pas votre milieu de travail ».

Comment accepter cela ? Sommes-nous prêts au Canada à laisser notre droit à la vie privée à la porte de notre bureau ? Le droit canadien confie aux gouvernements la responsabilité de certains droits fondamentaux de la personne ne pouvant être abolis par un contrat de travail. Le droit à la vie privée n'est pas encore du nombre. Le gouvernement fédéral a cependant prêté l'oreille et reconnu que la légalité était une chose mais que l'équité et la bonne gestion en étaient d'autres. Avec les nouvelles responsabilités qui incomberont sous peu au Commissariat, nous nous pencherons sûrement de plus près sur la vie privée en milieu de travail au sein des entreprises privées — tant la surveillance électronique que les questions biomédicales.

Technologie biomédicale

La technologie biomédicale s'est considérablement développée au cours des dix dernières années. Comme c'est si souvent le cas pour les nouvelles technologies, il s'agit d'une arme à double tranchant. Nous avons toujours poussé la population à s'interroger sur les bons comme les mauvais côtés de la technologie et à prendre leurs décisions en la matière sans perdre de vue certaines questions fondamentales relatives au type de société voulue.

La génétique n'aura bientôt plus de secrets : le séquençage de l'ensemble du génome humain est pratiquement terminé, bien plus tôt que prévu. Mais même si ces recherches permettent à la société d'espérer comprendre les composantes génétiques des maladies, elles menacent aussi de nous entraîner dans un tourbillon de renseignements extrêmement personnels, mal compris, pouvant mener à de nouvelles formes insidieuses de discrimination.

L'analyse de l'ADN (acide désoxyribonucléique) à des fins d'identification médico-légale constitue une percée tant pour les poursuites au criminel que pour disculper les innocents. Mais elle offre également la possibilité de créer des dossiers génétiques sur un grand nombre de citoyens.

Un recours croissant au dépistage antidrogue — moins marqué au Canada qu'aux États-Unis, mais tout de même important — a conféré à l'État et aux employeurs de nouveaux pouvoirs sans égal leur permettant de fouiller à leur gré les secrets de notre corps dans l'espoir d'y découvrir la preuve de comportements jugés inacceptables par la société.

Enfin, les mécanismes d'identification biométriques — des empreintes digitales numérisées aux technologies de reconnaissance des traits du visage en passant par les empreintes rétiniennes — ont transformé nos corps en codes d'identification. De plus, ces renseignements si intimes et indélébiles échappent à notre contrôle et deviennent accessibles à n'importe qui.

Dépistage génétique

Le dépistage et l'analyse génétiques pourraient très probablement nous permettre de rapidement détecter et traiter certaines maladies chez des personnes à risque. La génétique pourrait aussi aider les employeurs et les employés à améliorer la santé et la sécurité en milieu de travail en dépistant les affections génétiques susceptibles d'être aggravées par certains environnements. La surveillance des modifications et des affections génétiques en milieu de travail pourrait également permettre le dépistage et l'intervention précoces.

Cependant, le dépistage génétique pourrait causer beaucoup de torts. L'analyse génétique peut révéler des renseignements intimes et très délicats tant sur la personne examinée que sa famille. Lorsqu'on examine une personne, il existe des risques réels que les résultats servent à sélectionner et promouvoir les employés génétiquement aptes et à rejeter ceux qui sont inaptes, ou à déterminer qui est admissible aux avantages sociaux et aux assurances.

En 1992, nous avons déposé notre rapport intitulé *Le dépistage génétique et la vie privée*, qui dresse un tableau exhaustif des répercussions de cette nouvelle technologie sur la vie privée. La première de nos 22 recommandations demandait au gouvernement d'étudier l'ampleur du dépistage génétique au sein des organismes gouvernementaux et des entreprises privées, et les usages faits des renseignements ainsi recueillis. Nous recommandions également au gouvernement d'adopter une loi pour veiller à ce que le matériel génétique soit recueilli en fonction d'un cadre législatif, que personne ne soit obligé de fournir du matériel génétique, que le dépistage génétique ne soit pas une condition pour obtenir un emploi, et que personne ne fasse l'objet de discrimination pour avoir refusé de se soumettre au dépistage. Nous proposions également de modifier la définition de « renseignement personnel » de la *Loi sur la protection des renseignements personnels* pour qu'elle fasse référence tant aux échantillons de matériel génétique qu'aux renseignements découlant de leur analyse.

Le gouvernement est resté sourd à presque toutes nos recommandations, alors que chutent les coûts du dépistage génétique, s'allonge la liste des maladies que le dépistage peut identifier, et augmentent les pressions en faveur de bases de données médicales complètes et inter reliées sur chaque Canadien(ne). Nous ne disposons donc toujours pas de cadre législatif pour réglementer cette technologie si indiscrète, et nous ne connaissons même pas l'ampleur du dépistage génétique dans les bureaux canadiens, non plus que la méthodologie retenue par les employeurs.

Le dépistage génétique était l'un des enjeux pour la vie privée qu'a examiné le Comité permanent de la Chambre des communes sur les droits de la personne et le statut des personnes handicapées. Dans le rapport qu'il publiait en avril 1997, le Comité implorait le gouvernement d'intervenir sur-le-champ pour réglementer les atteintes à la vie privée et la discrimination découlant du dépistage génétique. Le Comité suggérait d'examiner les politiques et pratiques relatives au dépistage génétique dans les secteurs de l'emploi, de la santé, de l'assurance et de la justice pénale. De plus, il recommandait une révision des textes juridiques existants, des consultations publiques et une nouvelle loi pour contrer les atteintes à la vie privée et la discrimination.

Le Parlement a malheureusement été dissous peu après le dépôt du rapport du Comité, interdisant ainsi au gouvernement de réagir alors aux recommandations précédentes. Ces dernières ont cependant été reprises plus tard par le Comité permanent de la Chambre des communes sur le développement des ressources humaines et le statut des personnes handicapées, dans le cadre de son rapport sur le numéro d'assurance sociale. Malgré cela, le gouvernement a ignoré la question du dépistage génétique dans sa réponse à ce dernier rapport.

"SIGNEZ ICI, SOUFFLEZ ICI, APPOSEZ L'EMPREINTE DE VOTRE POUCE ICI, INSÉREZ UNE MÈCHE DE CHEVEUX ICI, UN ÉCHANTILLON DE SALIVE ICI, UN SPÉCIMEN ICI ET SOURIEZ."

Les enjeux de la génétique sur la vie privée ont fait couler beaucoup plus d'encre aux États-Unis. Un nombre important d'états ont adopté des lois interdisant la discrimination génétique en matière d'emploi et/ou d'assurance. Ce manque d'homogénéité juridique a cependant poussé certains députés fédéraux à parrainer des projets de loi imposant de semblables interdictions à l'ensemble des entreprises privées. En février 2000, le président Clinton a signé un décret interdisant au gouvernement fédéral d'obliger ses employés à subir des tests de dépistage génétique et de faire montre de discrimination génétique.

Analyse génétique à des fins médico-légales

Le dépistage génétique à des fins médico-légales est l'un des volets les plus

connus et populaires de la technologie biomédicale. Il a cependant des répercussions profondes sur la vie privée, car il consiste à prélever des substances corporelles sur des suspects ou des volontaires, à les analyser et à les comparer avec des éléments de preuve biologiques — peau, cheveux, sang ou sperme trouvés sur la scène d'un crime. L'analyse de l'ADN d'un suspect est ensuite comparée à celle de l'ADN trouvé sur la scène du crime. Les résultats peuvent soit innocenter le suspect soit établir une similitude relativement élevée (même si ce point est critiqué) entre les deux échantillons.

L'analyse génétique a été accueillie par tous comme la plus grande avancée en matière d'identification des criminels depuis le recours aux empreintes digitales. Technique relativement jeune et approximative au début des années 1990, elle a depuis acquis ses lettres de noblesse, notamment en innocentant David Milgaard et Guy Paul Morin, injustement emprisonnés. Moins spectaculaires mais plus sournoises, cependant, sont les pressions en faveur de la collecte et de l'entreposage de renseignements génétiques sur de grands pans de la population.

Nous appuyons le recours à un outil d'analyse à des fins médico-légales, mais nous opposons à sa transformation en un fichier national d'éléments biologiques d'identification. Nous nous inquiétons particulièrement de l'entreposage, non seulement des résultats d'analyse, mais aussi des échantillons analysés. La conservation de ces échantillons ne put pas faire autrement que d'inciter leur utilisation à des fins complètement différentes de recherche et autres. Des rapports américains révèlent une augmentation des pressions en faveur d'analyses supplémentaires des échantillons conservés pour pouvoir rajouter aux actuels marqueurs d'identification d'autres marqueurs permettant de préciser la race, le sexe, les caractéristiques physiques, les troubles psychiatriques possibles, etc.

Les premiers éléments de preuve génétique utilisés lors d'un procès canadien remontent à 1988, mais il a fallu attendre jusqu'en 1995, année où le Parlement a modifié le *Code criminel* afin de permettre le prélèvement de substances corporelles à l'aide d'un mandat, pour que soit créée une loi autorisant les agents de la paix à prélever des échantillons génétiques sur les suspects. Peu après, le Solliciteur général a entrepris des consultations au sujet de la création d'une base de données génétiques nationale visant à faciliter les enquêtes criminelles. La base de données contiendrait les échantillons provenant tant de la scène de crimes que de personnes reconnues coupables de diverses infractions, ainsi que leur analyse. Les documents de travail du Solliciteur général faisaient mention de plusieurs des enjeux pour la vie privée que détaillait *Le dépistage génétique et la vie privée.*

Nous avons demandé que la base de données se limite aux résultats d'analyse et ne comprenne pas d'échantillons biologiques. Nous avons également recommandé que les infractions visées par la base de données soient limitées aux infractions violentes pour lesquelles il serait possible d'obtenir des preuves génétiques. Toutefois, plusieurs groupes et de nombreux politiciens ont tenté d'obtenir le prélèvement automatique d'échantillons de toute personne accusée d'un acte criminel, au même titre que le prélèvement actuel d'empreintes digitales. Si leurs pressions avaient porté fruit, il serait aujourd'hui possible de prélever un échantillon (ne menant probablement à aucun élément de preuve) pour une infraction aussi « mineure » que le fait de signer un faux affidavit.

À son adoption en décembre 1998, la *Loi sur l'identification par les empreintes génétiques* comprenait sinon toutes, du moins certaines de nos recommandations. La base de données génétiques comprendra et l'analyse et les échantillons proprement dits, et les infractions visées seront plus nombreuses que nous ne le jugeons nécessaire. Néanmoins, bon nombre de nos recommandations ont provoqué l'ajout à la Loi de dispositions protégeant la vie privée, la plus importante étant l'interdiction (précisée dans des modifications ultérieures) d'utiliser du matériel génétique à des fins autres que l'identification médico-légale, réduisant ainsi le risque d'un détournement de finalités. Selon les modifications proposées à la fin de 1999, mais qui n'ont pas encore été adoptées, le Commissaire de la GRC devrait présenter chaque année au Solliciteur général un rapport sur les activités entourant la base de données génétiques, lequel serait ensuite déposé au Parlement. Un comité consultatif, auquel siègerait le Commissaire à la protection de la vie privée, surveillerait ces activités.

Nous félicitons le gouvernement de sa prudence face aux pressions importantes visant à élargir le prélèvement et l'analyse génétique à des fins médico-légales. À la fin de 1999, l'Association internationale des chefs de police, qui représente les services de police de 112 pays, a exhorté les assemblées législatives à adopter des lois exigeant le prélèvement d'échantillons de toute personne arrêtée, que ce soit pour meurtre, conduite avec facultés affaiblies ou vol à l'étalage. Au Royaume-Uni, la Lothian and Borders Police a lancé un programme de prélèvement d'échantillons de toute personne accusée d'une infraction, y compris d'infractions au code de la route.

Le plus grand danger que présente une base de données génétiques à des fins médico-légales est la possibilité qu'elle s'applique à une partie importante de la population, dont elle deviendrait alors un registre génétique. Retrouver les enfants kidnappés, aider les adultes amnésiques, assurer la sécurité des

personnes souffrant de la maladie d'Alzheimer : n'importe quelle raison serait bonne pour élargir le prélèvement d'échantillons, réduisant de ce fait l'écart entre les usages médico-légaux et ceux qui ne le sont pas.

Il y a plus de dix ans, alors que l'analyse génétique à des fins médico-légales n'en était qu'à ses balbutiements, l'universitaire américain Gary T. Marx, qui s'intéresse à la vie privée et à la surveillance, s'est penché sur cette nouvelle technologie, mettant en lumière le danger de ce qu'il appelait l'acceptation grandissante de la surveillance : l'acceptation progressive d'une grave atteinte à sa vie privée. Il se trouvera toujours de nouveaux usages pour tout système de surveillance jusqu'à ce que la nouvelle technologie nous plonge dans ce crépuscule si bien décrit par le juge américain William O. Douglas : « Tout comme la nuit, l'oppression ne tombe pas d'un coup. Dans un cas comme dans l'autre, entre chien et loup, rien ne semble changer. Et c'est là que nous devons tous être sensibles aux changements qui pourraient se produire — si légers soient-ils — pour ne pas devenir d'innocentes victimes de l'obscurité.» [traduction].

Dépistage antidrogue

Douze ans après avoir sonné pour la première fois l'alarme contre l'infiltration du dépistage antidrogue dans le milieu canadien du travail, nous n'avons pas changé d'idée. Cette forme de dépistage reste une grave intrusion dans la vie privée des gens qui n'est justifiée ni par le problème qu'elle se propose de régler, ni par son « efficacité » (laquelle reste à prouver). Un résultat positif à un test de dépistage antidrogue ne confirme ni l'affaiblissement actuel ou passé des facultés ni le risque d'un tel affaiblissement. Ce résultat n'indique pas non plus la quantité de drogue consommée ni le moment où elle a été consommée, et ne confirme même pas qu'il y a eu consommation. Tout ce que le résultat révèle, c'est que la personne visée a été en contact la drogue. Dans un même ordre d'idées, un résultat *négatif* à un dépistage de drogue ne permet pas non plus d'établir que la personne *n'a pas* consommé de drogue parce que les métabolites de drogue n'apparaissent dans l'urine que plusieurs heures après la consommation. L'éducation, le soutien et le traitement constituent les moyens les plus efficaces de contrer l'abus de drogue. Quelquefois, on peut aider les employés à régler leurs problèmes en améliorant leurs conditions de travail. Il vaut mieux aider les employés à reconnaître les risques associés aux drogues et à demander de l'aide plutôt que de tous les traiter comme des suspects.

Au début des années 90, le dépistage antidrogue constituait déjà un enjeu important pour la vie privée. Le décret qu'a présenté en 1986 le président Reagan visant le dépistage obligatoire et aléatoire des fonctionnaires fédéraux a donné le coup d'envoi à la vague de dépistage chez nos voisins du sud. Le

Canada n'a pas emboîté le pas aux Américains, malgré les insistances de divers intervenants du gouvernement et du secteur privé. Le Commissariat à la protection de la vie privée a réagi à leurs demandes en défendant la vie privée dans son rapport intitulé *Le dépistage antidrogue et la vie privée*.

À l'époque, Transport Canada proposait le dépistage antidrogue obligatoire et aléatoire des employés d'entreprises de transport terrestre, aérien et maritime. Le ministre de la Défense nationale, lui, annonçait qu'il effectuerait le dépistage obligatoire et aléatoire des membres des Forces canadiennes. Quant à Service correctionnel Canada, le dépistage était déjà une réalité pour les détenus des pénitenciers fédéraux. Notre rapport traitait de ces programmes, du dépistage antidrogue et de son bien-fondé, de la *Loi sur la protection des renseignements personnels*, et des répercussions plus vastes sur la vie privée.

Nous en concluions que les raisons invoquées pour justifier le dépistage antidrogue en général, et au dépistage obligatoire et aléatoire en particulier, ne résistaient pas à un examen approfondi. L'absence de preuves tant d'un problème de drogues que des bienfaits du dépistage sur la sécurité au travail ne justifiaient pas l'extrême intrusion que représente ce dernier.

Que notre rapport l'y ait poussé ou non, Transport Canada a abandonné son plan. Le gouvernement n'a rien proposé de semblable depuis et encore moins essayé d'étendre le dépistage antidrogue comme l'a fait le gouvernement américain. Les Forces canadiennes ont abandonné leur programme de dépistage aléatoire en 1995.

Ils se sont peut-être évité à tous bien des ennuis. Dans les années 90, le dépistage antidrogue a essuyé deux revers juridiques importants. En 1996, la commission d'enquête de la Commission ontarienne des droits de la personne a décrété que la politique de la Imperial Oil concernant les drogues et l'alcool violait le *Code des droits de la personne* de l'Ontario. En février 1998, la Division générale de la Cour de l'Ontario confirmait cette décision. L'appel qu'a interjeté la Imperial Oil en deuxième instance n'a pas encore été réglé. L'arrêté de la Imperial Oil revêtait une importance particulière puisqu'il visait le milieu de travail très dangereux d'une raffinerie de pétrole. Les tribunaux ont néanmoins décrété que l'entreprise pouvait veiller à la sécurité sans pour autant devoir recourir au dépistage antidrogue. En juillet 1998, la Cour d'appel fédérale a statué que la politique de dépistage des nouveaux et anciens employés de la Banque Toronto Dominion violait la *Loi canadienne sur les droits de la personne*. La Banque TD a depuis annulé cette politique.

Mais les pressions en faveur du dépistage antidrogue sont toujours aussi

fortes, en partie à cause de l'intégration accrue des économies canadienne et américaine. L'exemple le plus éloquent en est peut-être l'application en 1996 du règlement américain exigeant le dépistage antidrogue de tout camionneur, de quelque nationalité qu'il soit, conduisant sur les autoroutes américaines. Aujourd'hui, toute entreprise canadienne de camionnage qui emprunte à un moment donné une route américaine doit procéder à un dépistage antidrogue obligatoire et aléatoire. En 1998, apparemment inspiré par une loi américaine, un comité spécial du Sénat chargé d'examiner la sécurité dans les transports a recommandé les alcootests et le dépistage antidrogue aléatoire au Canada. (Le comité s'est dissous sans avoir déposé de rapport final. On ne sait donc pas quelle aurait été la réaction du gouvernement.)

Nous sommes ouverts à toute mesure visant à améliorer la sécurité publique. Si les tenants du dépistage antidrogue pouvaient prouver que ces programmes révèlent vraiment l'affaiblissement des facultés comme le font les alcootests, que les employés des transports sont aux prises avec un problème de drogue important ou que le dépistage antidrogue réduit les risques de façon importante, nos conclusions pourraient être différentes. Mais ce n'est pas le cas. Sans effets positifs manifestes sur la sécurité publique, le dépistage antidrogue ne peut que violer de façon humiliante la vie privée des travailleurs.

Le Canada n'a pas suivi la vague américaine. En 1996, selon une étude réalisée par la American Management Association, 81 p. 100 des grandes entreprises américaines administraient à leurs employés un test de dépistage antidrogue. Toutefois, nous avons remarqué que certains secteurs répètent la rhétorique américaine et joignent le geste à la parole : l'Ontario soumet les bénéficiaires de l'aide sociale à un test de dépistage antidrogue et impose le traitement obligatoire des personnes dont les résultats sont positifs. Cela s'inspire des programmes américains semblables, où la lutte antidrogue et la « démonisation » des bénéficiaires de l'aide sociale sont devenues des outils puissants de démagogie. Jusqu'ici, personne n'a décrié les tests auprès des tribunaux ontariens, mais cela pourrait fort bien survenir. Le droit ontarien considère que la toxicomanie est une incapacité, et qu'une personne souffrant d'une incapacité ne doit pas se voir refuser certains services comme les prestations d'aide sociale à cause de cette incapacité.

Un article satirique paru dans un numéro de 1998 du *Privacy Journal* proposait aux parents des lignes directrices sur le dépistage antidrogue de leurs enfants. L'une des difficultés, selon l'auteur, était que les enfants renversent la situation et fassent la même chose pour leurs parents. Sa solution : les parents devaient s'assurer de faire comprendre à leurs enfants l'importance de la communication et de la confiance dans la famille. Les personnes préoccupées

par la toxicomanie dans les écoles, les milieux de travail et la société, en général, devraient garder ce point, bien qu'ironique, à l'esprit.

Biométrie

Même s'il est encore trop tôt pour parler d'une révolution, nous avons été témoins d'une nouvelle tendance dans la façon de vérifier et d'authentifier l'identité des gens : avant, on se fiait à ce que l'on *possédait*, comme une carte, puis à ce qu'on *savait*, comme un mot de passe ou un numéro d'identification personnel (NIP) ; mais maintenant, on s'en remet à ce que l'on *est* : la biométrie.

C'est dans les années 70 que l'on a commencé à utiliser des technologies permettant de reconnaître et de mesurer des caractéristiques physiques ou comportementales comme les empreintes digitales, les traits du visage, les inflexions de la voix ou les particularités de l'iris ou de la rétine pour authentifier l'identité d'une personne. Cependant, pour la plupart des gens, la biométrie était presque de la science-fiction au début des années 90. Une série d'échecs essuyés dans les années 80 avait en effet poussé l'industrie à s'engager dans d'autres voies : claviers numériques, cartes d'accès et NIP.

Dans les années 90, on a cependant assisté à un regain d'intérêt pour la biométrie. En 1991, les ventes de dispositifs biométriques, à l'exclusion de ceux destinés aux forces de l'ordre, ont plus que doublé. L'augmentation de ces ventes est peut-être attribuable à la chute des prix. En 1995, selon un rapport de l'industrie, le « prix moyen pour un point d'accès protégé » a chuté à moins de 2 000 $, alors que, cinq ans auparavant, il s'établissait à plus de 6 000 $. Le rapport prédisait que les dispositifs de moins de 500 $ pourraient contribuer à faire de la biométrie une réalité de la vie quotidienne. En 1998, une entreprise américaine vendait des lecteurs d'empreintes digitales pour 99 $!

Avec la chute des prix, ce qui n'était auparavant qu'une utopie devient un besoin urgent : le rêve devient réalité. Il ne se passe pas une journée sans que soit proposée une nouvelle utilisation de technologies biométriques, des guichets bancaires à la police, en passant par la sécurité informatique, la gestion des prestations sociales et l'élimination. Presque chaque jour, nous entendons qu'il vient d'être inventé un nouvel usage des technologies biométriques — la monnaie électronique, le maintien de l'ordre, la sécurité informatique, l'administration des prestations sociales et la prévention de

l'école buissonnière.

Au début des années 90, le service américain d'immigration et de naturalisation a émis un nouveau document de voyage pour accélérer le dédouanement à l'aéroport international de Pearson, à Toronto : une carte à puce contenant la représentation mathématique de la forme de la main du titulaire, que des lecteurs électroniques situés dans l'aéroport pouvaient comparer à celle de la main de ce voyageur pour authentifier son identité. Il semble que l'on ait conçu cette technologie en tenant compte de la vie privée des voyageurs, puisque que l'image biométrique est mémorisée sur la carte, et non dans un ordinateur du gouvernement.

Plus tard dans la décennie, cependant, une application plus problématique a fait son apparition : les autorités de la région métropolitaine de Toronto ont décidé d'exiger que les prestataires d'aide sociale détiennent une carte à puce contenant leurs empreintes digitales numérisées. Ces cartes serviraient de porte-monnaie électronique pour leurs prestations d'aide sociale qu'ils pourraient ainsi dépenser directement dans les magasins. Comme nous l'avons fait remarquer dans un rapport antérieur, le problème de ce système tient en grande partie au fait qu'il peut mener à la constitution d'une base de données utilisables à des fins n'ayant aucun rapport avec les objectifs du système — par exemple, pour effectuer des recherches en sciences sociales sur les habitudes de consommation des prestataires d'aide sociale. En fin de compte, le système approuvé par toutes les municipalités n'utilise la technologie biométrique qu'à des fins d'identification et non comme une carte de débit, et comprend un certain nombre de dispositifs importants de protection de la vie privée. Mais le problème demeure : la prise d'empreintes digitales est associée depuis longtemps à la criminalité. Et, une fois de plus, on choisit de faire subir aux prestataires d'aide sociale un traitement qu'on ne réserve à aucun autre citoyen — et que peut-être aucun autre citoyen *ne voudrait* subir.

À la fin des années 90, la biométrie était sur toutes les lèvres. En décembre 1998, le *Globe and Mail* signalait qu'un centre de conditionnement physique de Toronto vérifiait l'admission de ses membres grâce à un lecteur des formes de la main et que Disney World utilisait un lecteur d'empreintes digitales pour identifier les détenteurs de laissez-passer annuels. Le *Globe* citait une source américaine, qui estimait à 500 millions de dollars les dépenses effectuées dans le monde entier l'année précédente pour l'achat de dispositifs biométriques. Au total, le tiers de ces ventes sont allées au secteur privé. Le *Globe* prédisait que les ventes de lecteurs d'empreintes digitales s'élèveraient à 1 milliard de dollars en 2001, alors qu'elles s'établissaient à 145 millions de dollars en 1997. Au début de l'année, le *Financial Post* relatait qu'une

entreprise australienne de technologie et d'investissement se préparait à lancer un dispositif de reconnaissance de la voix pour ses activités de commerce électronique. On y écrivait également que, bientôt, un système de reconnaissance de l'iris contrôlerait l'accès des employés à un aéroport américain, et qu'une banque canadienne commençait à utiliser des lecteurs d'empreintes digitales à des fins semblables. Une autre entreprise canadienne envisage de mettre au point une souris qui identifierait les empreintes digitales des utilisateurs voulant effectuer des transactions bancaires en ligne. L'aéroport international O'Hare, de Chicago, utilise des lecteurs d'empreintes digitales pour contrôler l'accès aux sections de manutention des bagages. Le *Post* mentionnait également qu'un hôpital américain a installé un système de reconnaissance des empreintes digitales permettant d'accélérer l'inscription des patients, d'éviter les demandes frauduleuses d'assurance et d'assurer au personnel de l'hôpital un accès immédiat aux dossiers médicaux des patients. La même entreprise fabrique un système qui contrôle l'accès aux ordinateurs en vérifiant les empreintes digitales.

Les défenseurs de la vie privée ont souvent attiré l'attention sur les répercussions qu'a la biométrie sur la vie privée : la collecte, l'utilisation et la conservation de renseignements personnels, et le potentiel qu'elle présente pour le couplage de différentes activités et transactions grâce à un élément unique d'identification. Mais le public n'a pas encore sérieusement réagi.

La technologie biométrique offre des avantages indéniables. L'authentification de l'identité, peu importe la façon dont elle le fait, est souvent cruciale, surtout à notre époque où de plus en plus d'entreprises transigent sur l'Internet. Contrairement aux mots de passe, un élément biométrique d'identification ne peut être ni donné, ni perdu ni oublié. Si la technologie peut faire en sorte que les maigres sommes allouées à l'aide sociale ne soient versées qu'aux personnes qui y ont vraiment droit, il est certain qu'elle aide les prestataires d'aide sociale plutôt que de leur nuire. Dans le très délicat contexte de la santé ou de l'aide sociale, un élément biométrique d'identification peut représenter un mécanisme très sécuritaire d'entreposage de données. Et qui peut s'opposer au contrôle de l'accès des employés, surtout en ce qui a trait à des activités cruciales sur le plan de la sécurité, comme les aéroports ?

L'exactitude de la biométrie, combinée à une chute des prix, peut devenir si attrayante que les gens peuvent décider de demander ou même d'exiger une preuve d'identité même lorsque cela n'est pas vraiment nécessaire. De nombreuses activités peuvent être effectuées de façon anonyme, comme le sont la plupart des transactions d'argent comptant. Il n'est pas toujours nécessaire d'identifier les gens. Comme c'est le cas des cartes d'identité (et de

tous les systèmes d'identification), nous devons éviter de laisser une nécessité occasionnelle mener à un usage facultatif généralisé pouvant provoquer de la suspicion et entraîner l'exclusion de personnes refusant de s'identifier lorsque cela est inutile.

Un autre problème lié à la biométrie est son intégration au système d'authentification exigé pour le commerce électronique, particulièrement l'infrastructure à clé publique. Le système entreposerait des caractéristiques biométriques auprès de « tiers de confiance », lesquels émettraient des certificats numériques de vérification de l'identité. Mais qui seront ces tiers ? Lorsque nous troquons notre vie privée en échange de sécurité — par exemple, lorsque nous donnons notre nom, notre adresse, notre numéro d'assurance sociale et d'autres renseignements personnels en échange d'un certificat numérique — nous ne pouvons déjà plus récupérer cette vie privée. Mais lorsque nous confions à d'autres personnes des marqueurs indélébiles, fixes et très personnels qui émanent de notre corps, le risque qui nous menace et le fardeau que porte celui qui les reçoit sont bien plus considérables.

La biométrie est intimement liée non seulement à l'identification, mais aussi à la surveillance. Il peut être devenir simple d'utiliser un lecteur d'empreintes digitales relié à un ordinateur pour vérifier si un employé commence réellement à travailler à une heure donnée. L'on pourrait même envisager un scénario encore plus envahissant : la technologie de la reconnaissance des traits du visage, qui sert à contrôler l'accès à certains lieux, est également à la base des systèmes de surveillance vidéo qui permettent de retrouver un visage dans une foule. En fait, la surveillance vidéo fait de la reconnaissance des traits du visage l'un des marchés de la biométrie qui connaît l'expansion la plus rapide. Selon le *Globe and Mail*, un système récemment mis au point permet aux organismes émetteurs de permis de conduire de retrouver un visage donné dans une base de données contenant un million et demi d'images. Et le *1997 Advanced Card and Identification Technology Sourcebook* indiquait, apparemment sans ironie ni désapprobation, que la même technologie de reconnaissance des traits du visage qui permettrait de détecter les terroristes dans les aéroports ou les fraudeurs d'aide sociale permettrait aussi à votre ordinateur multimédia de vous autoriser à participer à des téléconférences sur l'autoroute de l'information.

Réforme de la *Loi sur la protection des renseignements personnels*

La restructuration du gouvernement, les technologies de l'information de pointe et les technologies biomédicales mettent durement à l'épreuve l'efficacité de la *Loi sur la protection des renseignements personnels*, élaborée dans la période pré-technologique du début des années 1980. Même si la Loi a su

s'adapter à différentes réalités, elle s'essouffle de plus en plus. Nous avons essayé de l'ausculter et de rendre régulièrement compte des maux et des douleurs dont elle souffre, mais il est évident que les pansements ne suffisent plus et que la Loi a besoin d'une opération chirurgicale d'importance.

Il faut modifier la portée globale de la Loi pour qu'elle fasse bien ce que son nom indique. En 1998, nous avons entrepris d'examiner la Loi sous toutes ses coutures. Cet examen, que nous résumons plus loin dans ce rapport annuel, a été terminé à la fin de 1999 et a mené à plus de 100 recommandations visant à préparer la Loi aux défis de l'avenir. Puisqu'il en a terminé avec la Loi C-6, le Parlement doit maintenant revenir à son point de départ — protéger les renseignements personnels des Canadien(ne)s des bonnes intentions, sinon même du zèle, de l'État.

Loi C-6

Il semble judicieux de conclure ce survol des dix dernières années en commentant la *Loi sur la protection des renseignements personnels et les documents électroniques*, élément marquant du mandat du Commissaire. (Nous aborderons la Loi plus en détail plus bas.) Ces dernières années le Commissariat n'a pas cessé d'inviter le gouvernement fédéral à adopter une loi protégeant la vie privée des Canadien(ne)s dans le secteur privé. Maintenant que c'est chose faite, le personnel du Commissariat a hâte de s'attaquer aux nouvelles responsabilités que lui confère cette Loi.

Nous avons souvent répété qu'aucune des dispositions de la Loi n'est plus importante que celle qui demande au Commissaire à la protection de la vie privée de promouvoir la compréhension et la connaissance des enjeux reliés à la vie privée. L'un de nos objectifs sera donc d'informer les Canadien(ne)s de leurs droits et des dangers qui menacent leur vie privée, dont les conséquences personnelles et sociales des atteintes à leur vie privée. Nous souhaitons faire plus que simplement informer et éduquer : nous entendons faire du Commissariat à la protection de la vie privée l'organisme auquel la population peut faire appel lorsqu'elle se sent brimée dans ses droits à la vie privée.

Nous sommes tout aussi prêts à aider les entreprises privées. Nous savons qu'elles auront besoin de temps pour se familiariser avec la Loi, tout comme nous aurons besoin de temps pour nous familiariser avec les rouages du secteur privé. Il est normal que ces entreprises se sentent concernées quant à la manière dont la Loi les affectera et dont le Commissaire à la protection de la vie privée entend exercer son autorité. Nous ferons sûrement l'impossible pour ne pas entraver leurs opérations, mais nous ne voulons pas donner l'impression que rien ne changera. Nous nous attendons à ce que bon

nombre d'entreprises aient à rectifier leurs pratiques de gestion de l'information pour les rendre conformes à la Loi. Ce dont nous avons tous le plus grand besoin est un nouvel état d'esprit du monde des affaires face aux renseignements personnels. Ces derniers doivent être perçus comme plus qu'une simple ressource — quelquefois la ressource la plus importante de l'entreprise — dont l'entreprise ne sera jamais entièrement propriétaire. Le monde des affaires doit apprendre à devenir fiduciaire.

La loi C-6 : de l'ordre dans le secteur privé

Lorsque le Parlement a adopté la *Loi sur la protection des renseignements personnels et les documents électroniques*, le Canada a fait un pas de géant concernant la protection de la vie privée de ses citoyens. Cette loi clé hisse le Canada aux rangs enviables des principaux pays industrialisés qui ont reconnu la nécessité de légiférer en matière de protection des renseignements personnels dans le secteur privé.

Au cours des 20 dernières années, le public a manifesté un intérêt de plus en plus soutenu face à la protection de sa vie privée, intérêt provoqué par les changements sociaux, économiques et technologiques. L'expansion de l'économie mondiale, la prolifération des réseaux informatiques, la croissance exponentielle des transactions sur l'Internet, les télécommunications par satellite et les technologies de surveillance sophistiquées ont toutes contribué à l'inquiétude de la population et à son impression que sa vie privée est en train de disparaître.

La première réaction du gouvernement canadien aux demandes de protection des renseignements personnels — ou de protection des données, comme on l'appelle souvent en Europe — a été d'inclure dans la Partie IV de la *Loi canadienne sur les droits de la personne* de 1978 une disposition limitée sur la protection des renseignements personnels. Mais la Partie IV était loin d'être une loi exhaustive sur la protection des données ; elle portait essentiellement sur l'accès limité aux dossiers et ne prévoyait aucune mesure pour réglementer la collecte, l'usage et la communication des renseignements personnels du gouvernement. En 1982, le Parlement a promulgué la *Loi sur la*

protection des renseignements personnels, qui étendait la protection des renseignements personnels à presque tous les ministères fédéraux. Cette loi est entrée en vigueur le 1er juillet 1983.

En 1984, le Canada a, comme 22 autres pays industrialisés, adhéré aux *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* rédigées en 1980 par l'Organisation de coopération et de développement économiques. Ces lignes directrices visaient à harmoniser les lois et les pratiques en matière de protection des données des pays membres en établissant des normes minimales sur le traitement des données personnelles dans chaque pays. Les lignes directrices n'avaient pas force exécutoire, mais elles constituaient un repère et un point de départ pour créer des lois sur la protection des données dans un certain nombre de pays du monde entier.

Par l'adoption de la *Loi sur la protection des renseignements personnels* fédérale et ses équivalentes provinciales, le Canada a bien respecté son engagement d'établir au sein des gouvernements des pratiques équitables de gestion des renseignements personnels. Toutefois, avant que le gouvernement ne présente sa *Loi sur la protection des renseignements personnels et les documents électroniques* en 1998, rien ou presque ne protégeait le droit à la vie privée des Canadiens dans le secteur privé (sauf au Québec). La *Loi sur la protection des renseignements personnels et les documents électroniques* vient combler cette lacune.

Il aura donc fallu presque 20 ans au Canada pour étendre au secteur privé les pratiques équitables de gestion de l'information enchâssées dans les lignes directrices de l'OCDE et la *Loi sur la protection des renseignements personnels*. Le retard s'explique en partie par l'opposition du secteur privé, par le manque de volonté de la part du gouvernement, par l'incapacité d'arriver à un consensus sur la meilleure façon de protéger les renseignements personnels dans le secteur privé et par l'évolution du secteur technologique.

Poussé en partie par les lignes directrices de l'OCDE et peut-être par la crainte de ce qui pourrait découler de son inaction, le secteur privé a pris l'initiative dans les années 80 d'élaborer des codes de protection des renseignements personnels pour régler les préoccupations grandissantes relatives à l'usage détourné réel ou possible des renseignements personnels recueillis dans le cadre de transactions commerciales. En 1980, l'industrie de l'assurance vie a ouvert la voie en élaborant des lignes directrices sur le droit à la vie privée ; les banques, l'industrie du marketing direct, les sociétés informatiques et l'industrie des télécommunications lui ont emboîté le pas. Même s'ils ont été bien accueillis, ces codes sur la protection des renseignements personnels n'assuraient pas une protection complète; entre

autres, aucun organisme indépendant n'avait été mis en place pour surveiller leur application et traiter les plaintes des consommateurs.

Également de sa propre initiative, un comité de la CSA International (anciennement l'Association canadienne de normalisation) représentant l'entreprise privée, le gouvernement, les syndicats et les regroupements de consommateurs a débuté en 1991 un projet visant à élaborer un code type sur la protection des renseignements personnels qui ferait office de norme nationale minimale pour le secteur privé. S'inspirant des lignes directrices de l'OCDE, le comité a finalement convenu d'un code type préliminaire qu'il a fait circuler pour commentaire à la fin de 1994, puis approuver en 1996 par toutes les parties impliquées.

Même s'il appuyait le projet de la CSA et les autres initiatives volontaires, le Commissaire à la protection de la vie privée en est venu à croire qu'il n'était plus suffisant de faire preuve de bonne volonté. En 1992, il a exercé des pressions auprès de deux comités du Sénat en faveur de modifications à la *Loi sur les banques* qui habiliteraient le gouverneur en conseil à réglementer la collecte, l'usage et la communication des renseignements sur les consommateurs, et en faveur de l'intégration à la *Loi sur les télécommunications* d'un objectif stratégique de protection de la vie privée. Dans son rapport annuel de 1994-1995, le Commissaire à la protection de la vie privée prévoyait que le Code de la CSA pouvait revêtir toute son importance non pas sous sa forme proposée, en tant que code d'application volontaire à l'intention des entreprises, mais par son intégration à une loi-cadre nationale, norme nationale de protection de la vie privée que tous les secteurs devraient respecter.

Plusieurs faits nouveaux ont amené le Commissaire à croire qu'une loi exhaustive était nécessaire, notamment : les échanges commerciaux accrus de renseignements sur le consommateur ; la preuve de collectes, d'utilisations et de communications de renseignements sur les consommateurs à leur insu et sans leur consentement, et ce même dans des secteurs ayant adopté des codes de protection des renseignements personnels d'application volontaire ; les vastes écarts dans la protection assurée par ces codes d'un secteur industriel à l'autre ; l'absence prolongée d'un organisme de surveillance vraiment efficace dans ces secteurs ayant adopté de tels codes et, finalement, l'adoption, au Québec, d'une loi sur la protection des renseignements personnels dans le secteur privé.

En 1995, l'Association canadienne du marketing direct a exhorté le Parlement à rédiger une loi fondée sur le code type de la CSA. En réaction à la recommandation du Comité consultatif sur l'autoroute de l'information

d'établir des règles pour la protection des renseignements personnels dans le secteur privé, John Manley, ministre de l'Industrie, annonçait que le gouvernement fédéral déposerait une loi à cette fin. En 1996, Allan Rock, ministre de la Justice, réitérait cet engagement devant une assemblée réunissant les commissaires à la vie privée du monde entier, leur promettant qu'une loi régissant le secteur privé de compétence fédérale serait en place d'ici l'an 2000.

En octobre 1998, la *Directive sur la protection des données* de l'Union européenne entrait en vigueur. Cette Directive impose des normes en la matière pour tous les pays membres de l'UE, facilitant ainsi l'échange de renseignements personnels entre eux. Cependant, la Directive interdit aux pays membres de l'UE de procéder à de pareils échanges avec des pays externes à l'UE (dont le Canada) si ces derniers ne protègent pas les renseignements de façon adéquate.

Tous ces événements ont mené au dépôt par le gouvernement du projet de loi C-54, la *Loi sur la protection des renseignements personnels et les documents électroniques*, à l'automne 1998. Le projet de loi était l'un des jalons les plus importants de la législation canadienne en matière de vie privée. Il réglemente les usages commerciaux des renseignements personnels, exigeant des entreprises qu'elles respectent un code de pratiques équitables de gestion de ces renseignements. Une autre de ses importantes caractéristiques est qu'il investit un organisme indépendant de la tâche de surveiller les pratiques commerciales : le Commissaire à la protection de la vie privée doit en effet enquêter suite à toute plainte, présenter des rapports et mener des vérifications. En dernier recours, le projet de loi permet aux individus d'interjeter appel devant la Cour fédérale et habilite celle-ci à accorder des dommages-intérêts.

Enfin, le Commissaire devra remplir un mandat plus vaste : promouvoir la Loi en sensibilisant le public et en menant des recherches. Le Commissariat à la protection de la vie privée s'est toujours efforcé d'informer la population sur ses droits en matière de vie privée et les faits nouveaux qui renforcent ou menacent ce droit. Cependant, le Commissaire n'avait jamais encore été investi du pouvoir officiel d'éduquer le public. Le projet de loi corrige cette lacune et exige du Commissaire qu'il élabore et exécute des programmes pour amener le public à comprendre et à connaître les objectifs du projet de loi.

Le Comité permanent de l'industrie de la Chambre des communes a tenu des audiences exhaustives concernant le projet de loi au cours desquelles il a entendu près de 60 témoignages d'entreprises, d'associations, d'universitaires,

de consommateurs et de défenseurs de la vie privée. Les témoins tombaient dans l'une de deux grandes catégories : l'entreprise privée, qui trouvait le projet de loi trop contraignant, et les groupes de défense des droits civils et des consommateurs, qui jugeaient ce dernier trop laxiste. À l'issue des audiences, le Comité a présenté son rapport au Parlement. Il y formulait une bonne vingtaine de recommandations dont l'ajout d'une clause prépondérante et d'un test de raison, la nécessité de définir les « renseignements accessibles au public » dans un règlement, l'ajout d'exceptions permettant la communication de renseignements sans le consentement de la personne concernée, et la protection de dénonciateurs. Toutes les recommandations formulées par le Comité ont été acceptées par la Chambre.

Les députés fédéraux sont partis en vacances à l'été 1999 en laissant la *Loi sur la protection des renseignements personnels et les documents électroniques* à l'étape du rapport à la Chambre des communes. Au début de la nouvelle session, en octobre, le projet de loi a fait l'objet d'une mention dans le Discours du Trône et a été re-soumis à la Chambre sous le numéro C-6, toujours à l'étape du rapport.

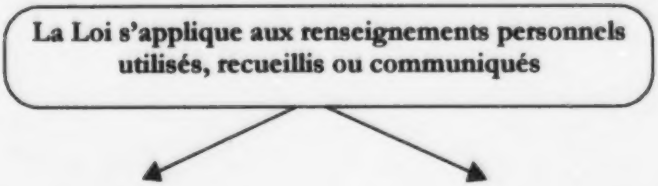
Les partis politiques représentés à la Chambre des communes ont déposé un nombre important de motions. Celles qui ont été adoptées excluaient les organismes d'enquête assujettissaient à la Loi l'échange et la vente de listes par des organismes sans but lucratif et précisaient l'application de la Loi au cours des trois premières années. Dans ce dernier cas, la Loi a été modifiée pour préciser qu'elle s'appliquerait également les trois premières années à toute entreprise provinciale communiquant des renseignements personnels à l'extérieur de la province pour contrepartie (notre emphase) La Chambre de communes a adopté le projet de loi ainsi modifié le 26 octobre 1999.

Ce dernier a ensuite été étudié par le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie. Le Comité a écouté beaucoup d'intervenants du secteur de la santé et a conclu qu'il s'agissait là du seul secteur qui n'appuyait pas le projet de loi. En fait, le secteur de la santé était lui-même divisé : certains intervenants recommandaient de resserrer les dispositions sur le consentement du patient et les usages subséquents de renseignements médicaux, alors que d'autres alléguaient que le projet de loi nuirait au fonctionnement du secteur de la santé. Face à l'opposition, le Comité a recommandé de reporter à un an suivant la date d'entrée en vigueur du projet de loi son application aux renseignements médicaux personnels. De cette façon, le secteur de la santé et les gouvernements disposent d'environ deux ans pour déterminer de quelle façon seront gérés pareils renseignements dans les activités commerciales.

En décembre, le Sénat a adopté le projet de loi avec cette modification, ainsi qu'une notion modifiée des renseignements médicaux personnels définissant ces derniers comme de l'information concernant la santé physique ou mentale d'un individu, mort ou vivant, et l'information recueillie lors de la prestation de services de santé à l'individu ou découlant de cette prestation. La définition porte aussi sur l'information concernant un don d'organe ou de substances corporelles, ainsi que l'information provenant d'examens médicaux. Ces modifications ont été entérinées par la Chambre des communes le 4 avril 2000.

Certaines entreprises se sont dites déconcertées par la Loi et par le rôle du Commissaire à la protection de la vie privée. Elles craignent de devoir consentir du temps ou de l'argent pour s'y conformer. Cependant, le Commissariat aidera les entreprises à s'adapter à la nouvelle Loi, et adoptera une approche prudente et impartiale face à son application. Il sera plus facile pour les entreprises de vivre la transition si elles gèrent soigneusement leurs renseignements personnels avant l'entrée en vigueur de la Loi, et qu'elles passent en revue leurs pratiques de gestion de l'information afin de respecter les normes établies dans la nouvelle Loi. Les entreprises qui pourront prouver qu'elles protègent les renseignements personnels de leurs clients éviteront leurs plaintes et gagneront leur confiance.

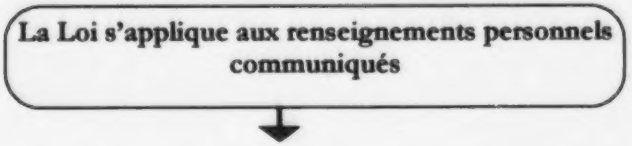
APPLICATION INITIALE DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*



Par une entreprise fédérale
Dans le cadre d'activités commerciales

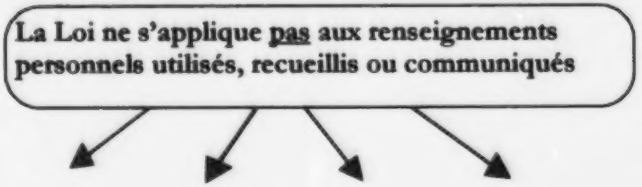
Par une entreprise fédérale
concernant ses employé(e)s

- Report d'application d'un an pour les renseignements de santé.



à l'extérieur de la province pour contrepartie

- Report d'application d'un an pour les renseignements de santé.



Par un individu à des fins personnelles

Par une organisation à des fins journalistiques, artistiques ou littéraires

Par une organisation à des fins autres que commerciales

À l'intérieur d'une province, sauf par une entreprise fédérale à des fins commerciales

Activité commerciale : toute activité régulière et tout acte isolé qui ont un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneur, d'adhésion ou de collecte de fonds.

Entreprise fédérale : relevant de la compétence législative du Parlement.

Perceptions canadiennes sur la vie privée : confiance et contrôle

Interroger les gens sur la vie privée présente un défi de taille : ceux que la question préoccupe le plus sont en fait les moins enclins à répondre, et bien des gens se sentent dérangés par les appels de maisons de sondage. De plus, il se peut que les personnes interrogées ne soient pas tout à fait conscientes de la diminution progressive de leur vie privée. Lorsque les secteurs public et privé utilisent des caméras cachées et des « cookies », apparient des données et interceptent les messages électroniques pour recueillir des renseignements personnels et surveiller leurs employés, leurs clients ou les citoyens, ils ne le crient pas sur les toits. Lorsqu'ils voient de leurs yeux que l'on viole leur vie privée, les gens le croient. Le problème, c'est qu'ils ne peuvent pas toujours le voir.

Malgré ces problèmes, les sondages restent le meilleur outil pour évaluer l'opinion publique. Le Commissariat à la protection de la vie privée a toujours manifesté un vif intérêt pour les attitudes des Canadiens face à leur vie privée, étant l'un des commanditaires du premier grand sondage sur le sujet, mené en 1992 par les Associés de recherche EKOS Inc, et intitulé *La vie privée exposée.*

En 1999, nous avons collaboré à un deuxième sondage d'EKOS, *Rethinking the Information Highway: Privacy, Access and the Shifting Marketplace.* Ce sondage portait sur un vaste éventail de sujets, dont la vie privée, l'accès aux technologies de communications, l'utilisation de l'Internet et la volonté des Canadiens d'utiliser ce réseau pour accéder aux services gouvernementaux. Ce sondage était en fait double : un premier échantillon aléatoire de 5 014 Canadien(ne)s âgés de 16 ans et plus a été interrogé en juin 1999, et un second de 1 830 (choisis au sein du premier) vers la fin de l'automne 1999. Les résultats sont considérés comme étant statistiquement exacts à plus ou moins 1,4 et 2,3 points de pourcentage dans 19 cas sur 20, respectivement.

En général, les Canadiens semblent moins préoccupés par leur vie privée qu'ils ne l'étaient en 1992. En 1999, 47 p. 100 des Canadiens croyaient avoir moins de vie privée au quotidien qu'ils n'en avaient il y a dix ans, par rapport à 60 p. 100 en 1992. La proportion de personnes croyant qu'il n'y a plus vraiment de vie privée parce que le gouvernement peut tout savoir sur les citoyens est passée de 81 à 63 p. 100. La proportion de Canadiens d'accord avec un énoncé semblable concernant les entreprises est passée quant à elle de 71 à 57 p. 100.

Les résultats du sondage de 1999 laissent croire que les Canadiens ont une perception plus affinée de la notion de vie privée. Cinquante p. 100 des gens interrogés croient qu'ils en savent désormais suffisamment pour prévoir les impacts d'une nouvelle technologie sur leur vie privée. Ils n'étaient que 42 p. 100 en 1992.

La majorité des Canadiens (54 p. 100) ne voit pas de problème à ce que les entreprises utilisent leurs renseignements personnels, du moment qu'ils le savent et qu'ils peuvent s'y opposer. La population semble prête à fournir des renseignements personnels dans certains cas et peut même vouloir sacrifier une partie de sa vie privée à condition de savoir ce dans quoi elle s'embarque.

Les Canadiens ont manifesté une volonté surprenante de troquer leurs renseignements personnels contre des avantages tangibles. Selon les résultats du sondage, 42 p. 100 des personnes interrogées accepteraient que les marchés d'alimentation surveillent leurs habitudes de consommation et dressent le profil de leur clientèle en échange d'un rabais de 10 p. 100 sur les produits qu'elles achètent. Un peu plus du tiers des internautes canadiens (36 p. 100) accepteraient qu'une entreprise reconnue surveille leurs habitudes de navigation en échange d'un nouvel ordinateur et d'un accès gratuit à l'Internet. Néanmoins, il vaut la peine de noter que ces avantages pourtant considérables ne suffisent pas à convaincre la majorité des Canadiens de vendre leur vie privée. L'hypothèse qui sous-tend ces deux questions est que les participants à de tels programmes savent pertinemment quels renseignements personnels on recueille et de quelle façon ils sont utilisés. Mais la réalité des programmes de fidélisation de la clientèle est tout autre.

Le sondage comprenait certaines questions connexes pour déterminer dans quelle mesure les Canadiens sont prêts à accepter des atteintes à leur vie privée qui faciliteraient certains objectifs publics tels de meilleures enquêtes criminelles ou une réduction de l'abus de programmes sociaux. Une infime majorité (51 p. 100) des réponses autorisent les gouvernements à apparier

leurs données des bases de données pour dépister les fraudeurs de l'aide sociale, alors que 44 p. 100 sont contre et croient que ce genre d'activité permettrait aux gouvernements de surveiller les citoyens. Soixante et un pour cent des personnes interrogées accordent aux forces de l'ordre le droit d'intercepter le courriel au cours d'enquêtes criminelles. Cinquante-cinq pour cent voient d'un bon œil le réseautage de leurs dossiers médicaux si cela permet d'améliorer la qualité des soins de santé. Par contre, le même pourcentage croit que les gouvernements recueillent plus de renseignements que ne le requiert la prestation de leurs services.

La volonté des Canadiens de fournir des renseignements personnels repose sur divers facteurs : leur compréhension du sort réservé à leurs renseignements personnels et de sa justification, leur confiance dans les organismes recueillant ces renseignements, et les avantages à en retirer. Les gens n'hésiteront peut-être pas à communiquer tels renseignements à telle entreprise, mais les refuseront à telle autre. Alors que seulement 19 p. 100 des Canadiens n'aiment pas l'idée de fournir des renseignements personnels aux médecins ou aux hôpitaux, la proportion monte à 27 p. 100 pour ce qui est des gouvernements, à 40 p. 100 pour les maisons de sondage et de recherche, à 49 p. 100 en ce qui a trait aux fournisseurs de services Internet, et à 62 p. 100 lorsqu'on parle des entreprises de télémarketing.

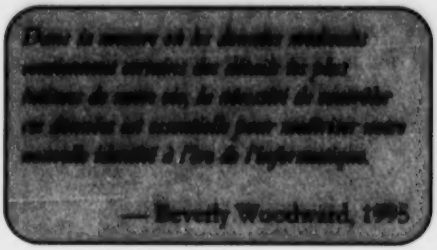
La volonté des Canadiens de fournir des renseignements personnels repose sur divers facteurs : leur compréhension du sort réservé à leurs renseignements personnels et de sa justification, leur confiance dans les organismes recueillant ces renseignements, et les avantages à en retirer.

Le sondage a révélé que les Canadiens sont préoccupés de façon importante par la capacité des entreprises et des gouvernements de protéger les renseignements personnels transigés sur l'Internet. À titre illustratif, la moyenne des internautes canadiens ne croit pas vraiment que les entreprises sont capables de pleinement protéger les renseignements personnels communiqués par réseau. Et seulement 12 p. 100 des Canadiens seraient prêts à donner leur numéro de carte de crédit via l'Internet lors d'un achat.

Que signifie tout cela ? Selon toute apparence, la vie privée reste une question complexe et beaucoup de Canadiens y tiennent, tout en se penchant davantage sur le volet sécurité de la question : ils veulent la protection de

leurs renseignements personnels. Cependant, les gens sont très divisés face à des initiatives gouvernementales qui compromettraient leur vie privée en échange de meilleurs soins de santé ou de services plus efficaces. Dans l'ensemble, plus de quatre Canadiens sur dix s'opposent au stockage de dossiers médicaux dans un réseau électronique protégé, même si cela améliorait les soins de santé. Le Commissariat à la protection de la vie privée croit que la faiblesse de la majorité appuyant de telles initiatives est une piètre excuse pour ne pas s'attaquer aux vrais enjeux, dont ceux pour la vie privée de notre population.

Renseignements médicaux : trop publics !



— Beverly Woodward, 1995

Patients et patientes assistent à l'érosion de leur droit à la vie privée au nom de la recherche, de la disponibilité de renseignements personnels et de l'efficacité administrative — et la population canadienne est la dernière à le savoir : un sondage mené récemment par l'Association médicale canadienne (AMC) révèle que trois personnes sur quatre croient que l'information donnée à leur médecin demeure confidentielle. La réalité est bien différente : une file longue et croissante d'intervenants attend derrière le médecin pour faire valoir ce qu'ils appellent un « besoin de connaître » ces renseignements.

Les renseignements personnels d'ordre médical stockés dans les systèmes électroniques deviennent de bonnes prises pour les bureaucrates, les chercheurs et les compagnies d'assurance ou de produits pharmaceutiques. De telles organisations récoltent et utilisent déjà clandestinement nos renseignements médicaux sans même avoir la courtoisie de nous informer que nos vies sont catégorisées et nos dossiers disséqués.

En outre, la technologie crée de nouvelles façons d'amasser sans notre consentement des renseignements sur notre santé. Par exemple, beaucoup d'internautes mènent aujourd'hui des recherches documentaires sur le Web au sujet de conditions et de traitements médicaux, pour des amis ou des parents. Qui aurait cru que beaucoup de sites Web reliés à la santé échangent les renseignements qu'ils recueillent de leurs visiteurs, malgré toutes leurs promesses de confidentialité ? C'est précisément ce qu'a révélé une recherche de la California Health Care Foundation, portant sur 21 sites Internet.

Il faut aussi accueillir d'un œil sceptique la prétendue protection promise avec la dépersonnalisation des renseignements médicaux. L'informaticienne américaine Latanya Sweeney a prouvé que le simple retrait du dossier médical d'un patient des données permettant de l'identifier ne suffisait pas à garantir la protection de leur vie privée, les renseignements restants ne donnant que l'illusion d'être anonymes. Selon Mme Sweeney, ces autres renseignements sont parfois si spécifiques, notamment quant aux traitements ou aux

maladies, qu'ils permettent de savoir quel patient ils visent. Il est également possible compléter ces autres renseignements par d'autres données, comme une date de naissance ou un code postal, pour identifier les gens par « divulgation inférentielle ».

Les chercheurs et les bureaucrates utilisent souvent un argument ahurissant : les patient(e)s, disent-ils, n'autoriseraient jamais l'utilisation en recherche de leurs renseignements personnels si on leur demandait leur consentement. Pourtant, des sondages actuels démontrent le contraire. En fait, le sondage de l'AMC révèle que près de huit Canadien(ne)s sur dix sont très ou assez d'accord avec la divulgation de leurs renseignements médicaux au gouvernement ou à des chercheurs, mais *uniquement* si on leur demande leur consentement. En l'absence de ce consentement, 51 p. 100 des Canadien(ne)s *refuseraient* la communication de leurs renseignements médicaux, même si les données permettant de les identifier en étaient retirées. Les gouvernements et les chercheurs sont invités à en prendre acte.

La confidentialité des patient(e)s est un élément crucial du succès des réseaux électroniques de santé, mais il semble qu'on doive constamment le rappeler aux promoteurs de tels réseaux. Malgré les nombreux avantages qu'elles laissent entrevoir, ces initiatives suscitent également des risques importants, y compris celui de propager des renseignements inexacts. La docteure Denise Nagel, directrice exécutive de la U.S. National Coalition for Patient Rights a fait l'observation suivante :

> « [L]es données obtenues par coercition ne sont pas fiables. Les patient(e)s qui savent que leurs dossiers de soins de santé seront examinés par des légions d'individus, connus ou non, ne diront pas la vérité. Ces personnes seront incitées à omettre des détails ou même à ne pas consulter du tout, si elles ont l'impression qu'une divulgation de renseignements confidentiels aurait des conséquences importantes. »

Jusqu'à très récemment, les patient(e)s se voyaient nier catégoriquement l'accès à leurs propres dossiers médicaux — il semblait inopportun de les laisser en savoir trop. Comme cette pratique semble offensante aujourd'hui ! Et pourtant, l'attitude actuelle témoigne du même préjugé : les patient(e)s n'auraient pas compétence pour décider de la divulgation de leurs renseignements médicaux à des fins de recherche.

Un des avantages les plus louangés d'un réseau d'information de santé consiste en de grandioses promesses de soins de santé améliorés. Pourtant les défenseurs d'un tel réseau offrent bien peu d'exemples précis de bénéfices concrets (outre la livraison quasi instantanée du dossier des patient(e)s aux

salles d'urgence). Il se peut bien qu'à la longue, des réseaux d'information de santé puissent contribuer à la qualité des soins de santé au Canada. Mais, à court terme, les risques pour la confidentialité des patient(e)s pèsent plus lourd que de tels avantages. Nous pouvons et devons éliminer ces risques — dont celui d'un échec de ces réseaux à cause de la méfiance du public si nous n'adoptons pas des garanties appropriées.

La confiance de la population dépendra des réponses que fourniront les organismes de soins de santé et les gouvernements à de nombreuses questions. Ils devront commencer par expliquer le détail des tierces personnes qui prendront connaissance d'un renseignement médical après que celui-ci a été communiqué par un patient à son médecin. Personne ne semble actuellement être en mesure de répondre aux demandes répétées en ce sens. En l'absence de détails sur la situation actuelle, il est donc difficile d'étudier à fond les incidences qu'un réseau d'information de santé aurait sur notre vie privée.

Il faudra aussi clairement définir notre terminologie. À titre d'exemple, il existe encore trop de confusion entre les notions de vie privée, de confidentialité et de sécurité, ce qui est critique. En effet, le respect de la confidentialité et de la sécurité n'équivaut pas au respect de la vie privée.

Notre droit à la vie privée est notre droit de ne pas être dérangés, de vivre sans obstacles, sans surveillance et sans intrusions. Ce droit humain est, selon un ancien juge de la Cour suprême, au cœur de la liberté dans un état moderne. Toute atteinte à notre vie privée est une atteinte à notre autonomie et notre liberté. Le respect de notre vie privée dans un contexte de santé pourrait bien tout simplement interdire la collecte de nos renseignements médicaux.

La notion de confidentialité implique une relation de confiance fiduciaire entre la personne qui fournit un renseignement et l'individu ou l'organisme qui le reçoit. Cette relation repose sur l'assurance que le renseignement ne sera pas divulgué sans le consentement préalable de la personne l'ayant fourni. La notion de confidentialité implique donc la communication initiale d'un renseignement.

La sécurité, quant à elle, repose sur des mécanismes technologiques ou administratifs visant strictement à empêcher la communication de renseignements confidentiels. Ici encore, l'on présume la communication initiale d'un renseignement.

D'autres définitions doivent être tout aussi claires : à preuve, ce terme de « collecteurs de données » que certains participants à une réunion, en mai 1999, sur le futur système national de surveillance de santé apposaient indifféremment à un gouvernement provincial, un laboratoire ou une régie de santé. D'autres personnes croyaient qu'il s'agissait plutôt du médecin de famille ! Jusqu'aux architectes mêmes de ces réseaux d'information qui ne se comprennent pas.

Et même lorsque nous aurons réussi à nous entendre sur la terminologie, il restera encore bien des enjeux à résoudre. Un des plus importants arguments à réfuter contestant l'aspect pratique de la notion de vie privée des patient(e)s est l'opposition au consentement. Donald Haines, de la American Civil Liberties Union, déclarait en 1996 que « les renseignements médicaux d'un patient sont son bras droit, et qu'un abus de ces renseignements auraient des conséquences pires que celles découlant d'un abus de ce bras. Nul ne devrait manier les renseignements d'un patient sans son consentement, pas plus que manier le bras droit de ce même patient sans son consentement » [traduction]. La confiance en un réseau d'information de santé passe par une protection par les gouvernements de la vie privée des patients. Notre dernier rapport annuel applaudissait la décision de consacrer des fonds de l'Inforoute canadienne de la santé à l'étude de la mise en application du code de protection des renseignements médicaux de l'AMC. Ce document, un « serment d'Hippocrate » de l'ère de l'information, est un excellent modèle à imiter, mais bien peu semblent intéresser à en tirer les importants enseignements qu'il contient en matière de protection de notre vie privée.

Même s'il est loin d'être aussi complet que le code de l'AMC, un récent projet de loi d'intérêt privé du député fédéral Greg Thompson va dans le bon sens. Sa *Déclaration des droits des patients* (projet de loi C-417) accorderait aux patient(e)s le droit d'examiner et de corriger leurs dossiers médicaux et, mieux encore, un droit à la confidentialité de leurs dossiers, à moins d'un consentement écrit et éclairé à leur divulgation. Le projet de loi incite à l'adoption d'une approche uniforme en assujettissant le financement fédéral

des soins de santé gérés par les provinces à la protection et la promotion des droits des patient(e)s.

N'oublions pas non plus le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie, dont les membres examinent actuellement la situation du système de santé au Canada et comptent présenter leur rapport final en décembre 2001. Le Comité se penchera sur les éléments suivants :

- les principes fondamentaux sur lesquels est fondé le système de santé publique ;
- l'évolution historique du système de santé ;
- les systèmes de santé publique à l'étranger ;
- les pressions et les contraintes du système de santé ; et
- le rôle du gouvernement fédéral dans le système de santé.

Le Commissaire à la protection de la vie privée a hâte de faire part de ses opinions au Comité.

Les instances chargées de l'élaboration de politiques publiques doivent s'assurer que les débats à venir sur la vie privée en matière de renseignements médicaux seront les plus ouverts et amples possible, ce qui permettra de faire avancer le projet. S'il leur faut un bon exemple de démocratie à l'œuvre, elles n'auront qu'à se pencher sur la préparation du rapport du Comité permanent de la Chambre des communes sur les droits de la personne et le statut des personnes handicapées publié en 1997 et intitulé *La vie privée : où se situe la frontière ?* Sous la présidence de l'honorable Sheila Finestone, les membres du comité ont dépassé la simple procédure, travaillant pendant près de 10 mois et faisant substantiellement avancer les connaissances et l'importance des questions de vie privée au Canada. Le comité débutait ses travaux voilà près de cinq ans, et il est permis de croire que certains des fonds de l'Inforoute canadienne de la santé pourraient subventionner un processus similaire de consultations sur la protection de la vie privée dans le domaine des renseignements médicaux. Un consensus ne se dégagera que suite à l'implication de toutes les parties : la population, les défenseurs des droits des patients et de la vie privée, les professionnels de la santé, les instances gouvernementales de soins de santé, les laboratoires, les pharmaciens, etc. Les patients qui sont la clé de ce réseau ne méritent rien de moins.

Progrès de l'inforoute canadienne de la santé, et protection des patients

Le Conseil consultatif sur l'infostructure de la santé a vu le jour en 1997 avec comme mandat de recommander au ministre de la Santé les éléments d'une stratégie qui mènerait à l'établissement d'une infostructure nationale de la santé. Le Conseil a cessé ses activités suite à la parution de son rapport final, en février 1999. Nombre des recommandations mises de l'avant par le Conseil plaisent au Commissaire à la protection de la vie privée. Comme nous l'indiquions l'an dernier, le Conseil a reconnu l'importance cruciale de la protection de la vie privée, et la considère comme un des quatre objectifs stratégiques de la construction du réseau. Le Conseil a également appuyé l'adoption de dispositions législatives particulières et en a défini les éléments essentiels. De plus, il préconise l'harmonisation des mesures de protection de la vie privée et a insisté sur le fait que cette harmonisation ne devrait pas tendre vers le plus petit dénominateur commun. Nous attendons impatiemment la réponse qu'Allan Rock, ministre fédéral de la Santé, fera à ce rapport final.

Le Commissaire à la protection de la vie privée a fait parvenir au ministre et au Conseil consultatif ses commentaires concernant le rapport final et le Carnet de route de l'information sur la santé, second document publié peu après le premier et visant la mise en œuvre du réseau. Le ministre a répondu que Santé Canada attachait beaucoup d'importance aux questions de protection de la vie privée et qu'un comité ministériel sur la protection des renseignements personnels sur la santé avait été créé pour veiller à ce que Santé Canada adopte une approche uniforme en matière de protection de la vie privée. En outre, il a indiqué que « la protection des renseignements personnels est une question de premier plan dans nos activités de réforme législative ». Ce sont de bien bonnes nouvelles ; si seulement nous pouvions être certains que la protection de la vie privée sera maintenue à un niveau élevé.

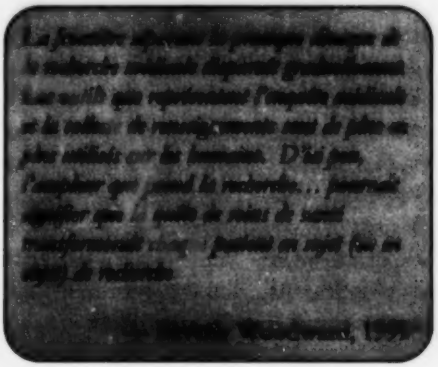
Malgré les assurances fournies par le ministre, l'Institut canadien d'information sur la santé (ICIS) et Statistique Canada ont, en janvier 2000, discrètement publié un nouveau et préoccupant document de mise en œuvre intitulé *Initiative du Carnet de route… Lancer le processus*, et tenu régulièrement à jour sur le site Web de l'ICIS à l'adresse http://www.cihi.ca.

Bien que disposant d'une charte fédérale, l'ICIS est un organisme indépendant sans but lucratif. Collaborant avec Santé Canada et Statistique Canada, son personnel centralise des programmes du Hospital Medical

Records Institute, du MIS Group, de la Division sur les renseignements de santé de Santé Canada, et de la Division sur la santé de Statistique Canada.

Le nouveau Carnet de route prévoit que l'ICIS se limitera à surveiller l'évolution des différentes juridictions impliquées et à réviser au besoin ses politiques et ses marches à suivre en matière de vie privée. Ce rôle d'observateur semble cependant aller à l'encontre tant des recommandations du Conseil consultatif en matière de vie privée que des assurances du ministre.

La plus récente version du Carnet de route résume quelque 36 projets actuels ou proposés. L'importance de la vie privée y est encore plus réduite que dans la version publiée l'an dernier comme compagnon au rapport final du Conseil consultatif (alors que cette question en était déjà pratiquement absente). La plus récente version fait notamment une nettement plus grande place aux « renseignements individuels » qui permettraient de suivre à la trace toute interaction entre une personne et le milieu de la santé, ainsi qu'aux renseignements déterminants provenant de sources autres que ce milieu. Si elle existe, la différence entre renseignements « individuels » et renseignements « personnels » nous échappe.



Le Carnet de route soulève plusieurs idées préoccupantes du point de vue de notre vie privée, dont :

- l'implantation d'un code national d'identification unique à chaque patient, centre de soins et professionnel de la santé ;
- la mise en place de normes nationales de déclarations d'usage (et d'abus) médicamenteux ;
- une collecte accrue de renseignements par les bureaux d'état civil ;
- une collecte accrue de renseignements par divers registres de maladies ou d'accidents.

Le Carnet de route indique que les enjeux de vie privée, de confidentialité et de sécurité seront traités dans le cadre du volet « infrastructure » du cadre stratégique de travail qui guide l'évolution du dossier.

Il est troublant de voir que l'inforoute sur la santé va de l'avant sans le minimum de protections pourtant recommandées au ministre par son propre Conseil consultatif. N'oublions pas non plus qu'aucune partie du budget de l'inforoute n'a été allouée à l'évaluation de l'effet de la mise en œuvre du code de protection des renseignements médicaux élaboré par l'Association médicale canadienne. De plus, nous attendons plus de détails sur les divers projets de l'Inforoute santé grâce auxquels nous pourrons évaluer les échanges d'information en cause. Après tout, à quoi sert d'étudier les risques que posent de tels échanges pour notre vie privée si nous ne connaissons même pas ces derniers ?

Comité consultatif sur l'infostructure de la santé et groupe de travail sur la vie privée

Contrairement à la passivité de l'ICIS et de Statistique Canada en matière de vie privée, les responsables fédéral, provinciaux et territoriaux de la santé ont déjà commencé à débattre activement de la question.

Le Regroupement des sous-ministres de la Santé bénéficie de l'appui du Comité consultatif sur l'infostructure de la santé, différent du Conseil consultatif précédent, désormais caduc. Le rôle de ce Comité mixte (fédéral, provincial et territorial) est de développer des stratégies nationales visant un recours accru aux technologies de l'information et des communications dans le secteur des soins de santé. Le Comité repose lui-même sur quatre groupes de travail — vie privée, surveillance, télé-santé et planification stratégique. Un cinquième groupe pourrait être créé qui examinerait les dossiers électroniques sur la santé.

Il semble que le groupe de travail sur la protection de la vie privée ait entrepris la négociation d'une « entente d'harmonisation » ou d'une « résolution » pour les sous-ministres de la Santé. Dans le cadre de cette résolution, chaque province et territoire se soumettrait à une auto-évaluation afin de repérer les lacunes au chapitre de la protection de la vie privée. Chaque gouvernement prendrait ensuite les mesures correctives qu'il juge nécessaires.

Il faut renforcer la protection, car la situation n'est pas rassurante. À titre d'exemple, une étude menée à la demande du gouvernement par la firme KPMG sur Pharmanet (le réseau informatique des dossiers sur les médicaments d'ordonnance des résidents) en Colombie-Britannique a révélé

que trop de gens ont accès à ces renseignements de nature confidentielle et délicate. Plus récemment, certains projets de SmartHealth au Manitoba, notamment la construction du Réseau d'information sur la santé, ont été remis en question suite à des allégations de mauvaise gestion. Dans un tel climat d'incertitude, on peut comprendre que les citoyens doutent que les gouvernements accordent la priorité à la protection de leurs renseignements médicaux.

Vu ces exemples, il serait sage que le groupe de travail sur la vie privée consultent les défenseurs de la vie privée avant d'adopter cette résolution. Nous attendons l'appel.

Réseau national de surveillance de la santé

Tel qu'indiqué ci-dessus, le groupe de travail sur la surveillance de santé se rapporte au Conseil consultatif sur l'infostructure de la santé.

Les intérêts du sujet individuel doivent toujours primer sur les intérêts de la science et de la société. [traduction]

— Déclaration de Helsinki de l'Association médicale mondiale, Recommandations aux médecins sur la recherche biomédicale impliquant des humains

En juin 1999, les sous-ministres fédéral, provinciaux et territoriaux de la Santé se sont réunis à Charlottetown et ont formellement proposé la mise sur pied d'un réseau de surveillance de la santé à l'échelle du Canada.

Le Commissaire à la protection de la vie privée a fait parvenir ses objections aux responsables de Santé Canada, s'opposant notamment à l'étude du style de vie de chaque individu, plus particulièrement des circonstances familiales, économiques, culturelles et sociales de chacun. Chaque Canadien(ne) doit pouvoir décider de participer à un tel réseau de surveillance de la santé, car il faut absolument préserver cette liberté de choix qui est une composante essentielle de la protection de notre vie privée. Cet argument a encore plus de poids lorsqu'on sait que ce réseau de surveillance va au-delà de la simple protection du public contre des menaces pour sa santé : en effet, le réseau se propose également de promouvoir la bonne santé et le bien-être.

Santé Canada a créé un site Web portant sur ce réseau de surveillance et visant à informer la population. Les personnes intéressées peuvent également obtenir le bulletin électronique du réseau, *HealthSurv.news*, à l'adresse health_surveillance@hc-sc.gc.ca ou en composant le 1-888-288-2098.

La loi albertaine sur les renseignements en matière de santé — Qu'en est-il au juste ?

La nouvelle *Health Information Act* de l'Alberta (connue antérieurement sous le nom de projet de loi 40) a reçu la sanction royale le 9 décembre dernier. La Loi donne aux individus le droit d'accès à leurs renseignements personnels médicaux, établit des règles pour la collecte, l'utilisation et la communication de ces renseignements et prévoit un mécanisme d'examen indépendant par le Commissaire provincial à l'information et à la vie privée.

Bien qu'elle soit moins exhaustive que la *Health Information Protection Act* de la Saskatchewan (adoptée l'an dernier), la loi albertaine exige que tout « gardien » (personne ou organisme qui contrôle des renseignements personnels) qui veut communiquer par des moyens électroniques des renseignements sur un diagnostic, un traitement ou des soins concernant une personne identifiable doit d'abord obtenir le consentement de cette personne. Compte tenu de la popularité des dossiers médicaux électroniques et de la création du réseau albertain we//net — qui intègre les renseignements provinciaux en matière de santé — nous espérons que les dispositions permettant aux patients de contrôler l'informatisation et le réseautage de leur dossier médical prendront de l'importance.

Le Commissaire albertain à l'information et à la vie privée, Robert Clark, a examiné la Loi et, bien qu'il ne s'y oppose pas, a cerné plusieurs problèmes. En fait, selon M. Clark, le projet de loi 40 n'est pas une loi sur la protection de la vie privée, mais plutôt une loi d'accès à l'information qui permet la communication de renseignements dans un certain nombre de conditions. D'ailleurs, plusieurs groupes, dont la *Alberta Medical Association* (AMA), se sont nettement prononcés contre le projet de loi 40. Les raisons de l'opposition de l'AMA étaient les suivantes :

- le projet de loi ne respecte pas la norme du *Code de protection des renseignements personnels sur la santé* de l'Association médicale canadienne, code approuvé par l'AMA ;
- il change fondamentalement la relation médecin-patient ;
- il compromet la capacité des médecins de conserver les dossiers de leurs patients dans leurs cabinets ;

- il élargit la notion de consentement du patient de simples raisons thérapeutiques à une vaste gamme d'activités non directement liées aux soins médicaux du patient.

Les médecins ont soulevé d'importantes préoccupations. La Loi n'exige pas toujours le consentement des individus pour la collecte, l'utilisation et la communication des renseignements personnels concernant leur santé : deux des 17 exceptions stipulent notamment que le consentement n'est pas requis si cela permet de minimiser ou d'éviter un danger imminent qui affecterait la santé ou la sécurité de quiconque ou si cela permet de détecter ou d'éviter un abus frauduleux du système. De plus, la Loi ne s'applique pas à certaines entreprises privées telles les compagnies d'assurance, et aucune interdiction ou sanction n'est prévue pour la collecte ou l'utilisation du numéro d'assurance maladie à des fins non liées à la santé. En outre, le ministre, son ministère, une autorité régionale de santé, le *Provincial Health Board* et le *Alberta Cancer Board* ont le pouvoir non seulement d'exiger de tout gardien que ce dernier leur remette n'importe quel renseignement médical identifiant sa source, mais aussi de divulguer ces renseignements à n'importe quel autre gardien.

L'un des aspects les plus inquiétants de la nouvelle loi albertaine est qu'elle permet à n'importe quel gardien d'établir les antécédents familiaux ou génétiques d'une personne pour n'importe quelle raison, sans demander aux patients leur consentement ni même les informer de cette pratique. L'objectif semble être une collecte massive et un stockage généralisé de renseignements qui serviront peut-être un jour sans restrictions à un quelconque chercheur. Ce suivi effréné de renseignements personnels est particulièrement troublant. Quelles sont les limites, s'il y en a, quant aux types de renseignements qui pourraient intéresser les chercheurs ? Des groupes de citoyens — des familles entières et leurs descendants pendant des générations — peuvent être stigmatisés par des bureaucrates du domaine de la santé, des compagnies d'assurance ou des employeurs qui se serviraient contre eux de renseignements personnels concernant leur santé.

Sûrement très révélatrice de l'objet et de l'esprit de cette nouvelle *Health Information Act* albertaine est la suppression du mot « protection » de son titre (lequel se lisait *Health Information Protection Act* en 1997). Un nouveau titre qui en dit long…

Un numéro permanent d'identification pour les médecins

Les étudiants en médecine, les internes et les médecins du Canada se verront bientôt attribuer un nouveau numéro d'identification à vie. Selon les organismes qui mettent le système au point (la Fédération des ordres des médecins du Canada, le Conseil médical du Canada et l'Association des facultés de médecine du Canada), le numéro à neuf chiffres ne permettra d'identifier que le médecin. Il ne contiendra pas d'autre information codée, comme la spécialité ou le statut d'agrément. Les organismes ci-dessus avancent que ce numéro d'identification est nécessaire parce qu'on a de la difficulté à identifier les médecins de façon exacte. L'attribution des numéros d'identification débutera dans plusieurs provinces en avril 2000.

Même si nous avons demandé à la Fédération de se raviser et de prendre d'autres mesures administratives pour identifier les médecins, nous la félicitons de nous avoir d'abord demandé notre avis. Le fait de demander l'opinion des responsables de la vie privée sur ce type de projet démontre une sensibilité à la question que d'autres organisations feraient bien d'adopter. Il reste à savoir dans quelle mesure nos commentaires ont influé sur la proposition originale.

Nous avons fait plusieurs suggestions. Par exemple, l'expérience a montré que les renseignements personnels présentés dans une forme accessible peuvent subir des détournements de finalités. Même si le système est doté d'un mécanisme de protection, la seule existence du numéro suscitera de nouveaux usages sans rapport avec les fins premières. Lorsqu'on aura attribué un numéro à tous les étudiants en médecine et à tous les médecins, il se pourrait qu'on tente d'accéder sans autorisation à leurs renseignements personnels à l'aide de ce numéro. Et lorsque de nombreuses organisations utilisent un numéro d'identification commun, la possibilité que les renseignements provenant de sources disparates soient compilés en un profil global augmente. Les numéros d'identification personnels uniques et les technologies puissantes peuvent sembler régler les problèmes administratifs immédiats, mais, à long terme, ils menacent la vie privée de chacun, valeur fondamentale d'une société démocratique.

Réforme de la *Loi sur la protection des renseignements personnels*

Lors de la rédaction de la *Loi sur la protection des renseignements personnels* (la *LPRP*) fédérale en 1982, le gouvernement prévoyait passer la Loi en revue périodiquement pour s'assurer qu'elle demeure pertinente et efficace. D'où l'article 75, qui stipule que le Parlement doit examiner la Loi trois ans après son entrée en vigueur et, par la suite, de façon permanente. En 1986, le Parlement a examiné la *LPRP* et la *Loi sur l'accès à l'information* en détail, publiant l'année suivante le document intitulé *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*. Ce document formulait plus de 100 recommandations pour l'amélioration de la Loi, mais aucune d'entre elles n'a été retenue. Toutefois, plusieurs recommandations ont donné lieu à des directives stratégiques, notamment celles sur le couplage des données et sur la restriction de l'usage du numéro d'assurance sociale par le gouvernement.

Il y a maintenant plus de dix ans que le Parlement s'est penché sur la *LPRP*. En 14 ans, le monde de l'information a été littéralement transformé par l'Internet, l'identification par les empreintes génétiques (et autres biotechnologies), l'entreposage des données et la réduction des effectifs au gouvernement. Certains de ces facteurs mettent en péril les assises de la Loi. Nous ne nous sommes jamais gênés pour en signaler les faiblesses ; tout au long des années 90, le Commissaire à la protection de la vie privée a recommandé d'apporter de nombreux changements à la Loi. Aucune de ces recommandations n'a été adoptée, et les lacunes de la Loi grandissent.

Ces faiblesses sont encore plus évidentes depuis l'adoption par le Parlement de la *Loi sur la protection des renseignements personnels et les documents électroniques* (Loi C-6). Cette Loi (qui réglemente le traitement des renseignements personnels dans le secteur privé) comprend beaucoup de caractéristiques supérieures à la *LPRP*, ce qui rend l'examen exhaustif de cette dernière à la fois urgent et inévitable.

Nous avons donc commencé à analyser la Loi en profondeur afin d'élaborer une série de recommandations concrètes de modernisation et d'amélioration. L'examen a pris fin en décembre 1999 et a permis de formuler plus de 100 recommandations. Nous vous présentons ici les plus importantes ; le rapport complet sera accessible d'ici l'été 2000.

Accorder la primauté à la Loi
Même si le Commissariat allègue que la *LPRP* est une loi prépondérante, étant donné qu'elle défend un droit fondamental de la personne, le libellé de la Loi est beaucoup moins clair à ce sujet. Dans la réalité, les institutions fédérales peuvent souvent violer les droits à la vie privée des citoyens lorsqu'une autre loi le permet ; la *LPRP* n'a pas préséance. Ironie du sort : lorsque la protection de la vie privée relevait de la *Loi canadienne sur les droits de la personne*, loi d'application générale, elle jouissait d'un statut quasi constitutionnel qu'elle semble selon toute apparence avoir perdu aujourd'hui. Le temps est venu de corriger la situation et de redonner au droit à la vie privée la place qui lui revient au sein des valeurs fondamentales qui sous-tendent notre société libre et démocratique. La *LPRP* devrait clairement stipuler sa primauté sur toute autre loi traitant de la collecte, de l'usage et de la communication de renseignements personnels.

En faire une vraie loi sur la vie privée
La *LPRP* ne porte que sur la protection de l'information. Mais il devient de plus en plus évident que l'État viole la vie privée des gens sans pour autant avoir besoin de recueillir des « renseignements personnels » tels que définis dans la Loi : prenons la surveillance électronique en temps réel du comportement des gens, qui ne mène pas nécessairement à la création d'un « dossier », et le prélèvement de substances corporelles, qui ne constituent pas de prime abord des renseignements personnels. Ni l'une ni l'autre de ces pratiques ne sont réglementées par la Loi actuelle.

Ces formes de violation de la vie privée ne devraient pas plus échapper au contrôle de l'État qu'une autre forme de collecte de renseignements. Nous recommandons que la définition de « renseignement personnel » de la *LPRP* reflète celle de la nouvelle Loi C-6, qui ne se limite pas aux renseignements « enregistrés ».

Préciser les communications de renseignements sur les fonctionnaires
Les droits à la vie privée des fonctionnaires fédéraux nourrissent depuis longtemps les débats entre les défenseurs du droit à la vie privée et les tenants du droit du public de savoir de quelle façon le gouvernement gère les affaires de l'État. La *LPRP* considère que les renseignements portant sur le poste ou les fonctions d'un fonctionnaire ne sont pas « personnels ». Ainsi, ils ne sont pas protégés par les dispositions sur l'usage et la communication (articles 7 et 8) de la *LPRP*. Nous ne remettons pas en question l'importance du droit du public d'obtenir des renseignements sur les activités du gouvernement, y compris certains renseignements personnels sur ses employés. La Loi pourrait cependant établir un meilleur équilibre entre l'intérêt du public à recevoir des comptes du gouvernement et la vie privée

des fonctionnaires en définissant plus clairement ceux des renseignements personnels concernant un employé qui peuvent être communiqués.

Classer les communications de renseignements : avec ou sans avis
La Loi est déficiente quant aux obligations qui incombent à une institution fédérale en matière de communication de renseignements personnels, visée par une longue liste au paragraphe 8(2). Ce dernier autorisant les communications sans le consentement de la personne concernée, la Loi devrait en contrepartie imposer aux institutions fédérales l'obligation d'informer cette personne de la communication. Il va de soi que certaines dispositions sur la communication ne peuvent être liées à une obligation d'informer l'individu avant la communication de renseignements (par exemple, la communication de renseignements aux autorités policières aux fins d'enquêtes criminelles). Mais l'on ne peut pas en dire autant de toutes les communications permises. Qu'y aurait-il de mal à informer des individus du fait que des renseignements les touchant ont été communiqués aux Archives nationales à des fins historiques ? Les dispositions relatives à la communication de renseignements devraient être séparées en deux catégories : celles pour lesquelles il est pratique et raisonnable de fournir un avis préalable, et celles n'exigeant pas que l'individu le sache.

Pourquoi faudrait-il aviser les gens au préalable si le gouvernement peut communiquer des renseignements personnels sans leur consentement ? Certains allèguent qu'un préavis n'est guère utile si l'on ne peut rien faire pour empêcher la communication. Toutefois, l'avis préalable permettrait aux gens de contester une communication de renseignements avant que celle-ci n'ait lieu. Dans son rapport annuel de 1991-1992, le Commissaire à la protection de la vie privée faisait remarquer que la *Loi sur l'accès à l'information* fournit un mécanisme pour alerter les tiers, comme les entreprises, que des renseignements commerciaux confidentiels sur eux pourraient être communiqués. Cependant, la *LPRP* ne confère aucun droit de ce genre aux personnes dont les renseignements personnels confidentiels pourraient être communiqués. Les renseignements personnels ne méritent-ils pas d'être protégés des abus de la même façon que ne le sont les renseignements commerciaux ? Cette question reste toujours sans réponse.

Lorsqu'un avis préalable est requis, les institutions fédérales devraient ne pas pouvoir communiquer de renseignements personnels avant que la personne n'ait eu la possibilité raisonnable d'y consentir ou de s'y opposer (à moins que le fait de ne pas communiquer les renseignements immédiatement ne cause un tort précis). L'institution pourrait communiquer les renseignements même si la personne s'y oppose, à moins que celle-ci n'ait demandé à un tribunal de se pencher sur la question. En pareil cas, comme le prévoit la *Loi sur l'accès à*

l'information fédérale, l'institution fédérale devrait suspendre sa décision jusqu'à ce que le tribunal ait examiné la cause.

Confier au Commissaire à la protection de la vie privée toutes les plaintes relatives aux renseignements personnels

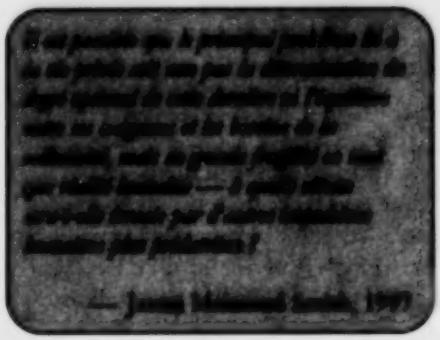
L'article 19 de la *Loi sur l'accès à l'information* exige que le gouvernement refuse la communication de documents contenant des « renseignements personnels » visés par la *LPRP*. Ainsi, la communication n'est possible que si cette dernière Loi le permet. Toutefois, le Commissaire à l'information étudie maintenant les plaintes selon lesquelles le gouvernement a refusé à un tiers l'accès à des documents parce que les renseignements qui y figurent sont « personnels », vérifiant de ce fait l'application de la *LPRP*. Le Commissaire à la protection de la vie privée se borne à être avisé d'une situation où la communication des renseignements est faite dans l'intérêt public ou à recevoir les plaintes des personnes s'opposant à la communication. C'est là que le bât blesse : un organisme dont le mandat est de promouvoir l'accès aux documents gouvernementaux interprétant une *LPRP* qui vise à empêcher le public d'avoir accès à des renseignements personnels.

La recommandation ne vise pas à critiquer l'intégrité ou la compétence du Commissaire à l'information ni à usurper de quelque façon que ce soit le rôle d'ultime arbitre de la loi qu'assument les tribunaux. Néanmoins, si le gouvernement communique des renseignements personnels en réponse à une demande d'accès, le Commissaire à la protection de la vie privée devrait pouvoir se pencher sur n'importe quelle plainte visant de tels renseignements.

Élargir les recours aux tribunaux

L'une des plus vieilles critiques à l'endroit de la *LPRP* fédérale actuelle vise le peu de recours juridique qu'elle confère aux gens : ceux-ci ne peuvent en effet contester devant les tribunaux que les refus d'accès à leurs propres renseignements personnels. Et même dans ce cas, le tribunal ne peut qu'ordonner la communication des renseignements demandés s'il est d'avis que le refus initial n'était pas fondé. Cette limite est inacceptable en termes des droits à la vie privée de la population. Le droit d'accéder à ses propres renseignements personnels, même s'il est important, n'est qu'un des nombreux droits qui permettent aux gens d'exercer un certain contrôle sur la façon dont le gouvernement traite les renseignements qui les concernent. Les restrictions qui s'appliquent à la collecte, à l'usage et à la communication des renseignements par le gouvernement sont des principes tout aussi importants — sinon plus — qui sous-tendent toute loi sur la protection des renseignements personnels.

La nouvelle Loi C-6 donne aux individus le droit de demander aux tribunaux de réviser toute décision d'une entreprise en matière de collecte, d'utilisation et de communication de renseignements personnels, ainsi que de leur accès par la personne concernée. La Loi permet également aux individus lésés de réclamer des dommages-intérêts pour toute conséquence adverse résultant de manquements à la Loi. La disparité entre cette Loi et la *LPRP* est clairement indéfendable : le public aurait moins de droits face au gouvernement lorsqu'il traite avec le gouvernement qu'il n'en aurait face au secteur privé ! Il faut modifier la *LPRP* pour élargir les questions que le tribunal peut examiner et les recours qui s'offrent aux plaignants.



Intégrer des règles sur le couplage de données

La *LPRP* ne contient aucune règle précise régissant le couplage des données. Même si le Conseil du Trésor a établi en 1989 des lignes directrices à ce sujet, ces dernières ne constituent qu'une directive stratégique et n'ont pas force de loi. Elles exigent que le ministère pilotant le couplage soumette une proposition détaillée pour examen par le Commissaire à la protection de la vie privée. Vu le peu de propositions qui nous ont été soumises, nous soupçonnons depuis longtemps que la plupart des activités de couplage de données ne sont pas déclarées, et qu'elles ne sont donc portées à la connaissance ni du Commissaire ni — fait plus important — du public. Si la Loi incorporait l'obligation de déclarer tout couplage, les institutions fédérales devraient s'y conformer ou subir les conséquences.

Le faible nombre des déclarations que le Commissariat a reçues est peut-être attribuable à une simple négligence. Il se peut également que les fonctionnaires ne définissent pas l'activité qu'ils prévoient comme un couplage de données, ce qui soulève des questions au sujet de la clarté de la directive stratégique. En général, un couplage de données se définit comme une comparaison de renseignements personnels recueillis auprès de diverses sources à des fins différentes. Cela comprend les couplages de données visant à confirmer que les renseignements contenus dans une base de données correspondent à ceux d'une autre base. Il est fort probable que les bureaucrates ne reconnaissent pas cette activité de confirmation comme étant

un couplage de données. Même si pareille activité est moins susceptible de violer la vie privée des gens lorsqu'ils en sont avisés, elle constitue quand même une forme de couplage et doit être signalée.

Toutefois, le couplage de données peut générer des renseignements autres que la simple confirmation d'équivalences entre diverses bases de données. Il peut créer de nouveaux renseignements jusqu'ici inconnus sur une personne et qui ne sont apparents dans aucune des bases de données utilisées. Cette forme de couplage de données viole davantage la vie privée si on recueille des renseignements indirectement à l'insu et sans le consentement de la personne concernée. Tout cela fait ressortir l'importance cruciale de mieux connaître et de davantage contrôler les couplages de données, ainsi que d'étudier leurs impacts sur la vie privée, éléments qui brillent par leur absence dans la politique actuelle sur le couplage de données et qui gagneraient à être incorporés dans la Loi pour mieux guider les institutions fédérales.

Contrôler les données contenues dans les registres publics

Les dispositions sur l'usage et la communication qui se trouvent dans la Loi ne s'appliquent pas aux renseignements personnels « auxquels le public a accès ». La signification exacte de cette dernière notion a fait l'objet d'un débat houleux depuis l'adoption de la Loi. Petit à petit, deux explications se sont dégagées : la première, lorsque l'individu accorde son consentement exprès ou implicite à la communication, et la seconde, lorsque la Loi exige que les renseignements soient mis à la disposition du public. Cette dernière explication provoque des problèmes importants au sujet de la protection des renseignements personnels.

Les exemples les plus fréquents de renseignements personnels mis à la disposition du public comprennent les registres gouvernementaux tels le Registre des faillites ou le Registre des groupes de pression. Bien qu'il soit justifié de mettre pareils renseignements à la disposition du public, peu de registres gouvernementaux, voire aucun, contrôlent la quantité et la nature des renseignements qu'ils communiquent, non plus que les usages qui peuvent en être faits une fois communiqués : il n'y a qu'à penser à l'implantation de registres publics sur l'Internet et à la communication de renseignements en vrac à des fins de marketing, deux gestes auxquels le gouvernement n'avait sûrement pas pensé lors de la création des registres. Les institutions gouvernementales ne devraient jamais communiquer de renseignements personnels provenant d'un registre gouvernemental à des fins autres que celles pour lesquelles le registre a été établi. Elles ne devraient pas non plus divulguer l'ensemble des données du registre, ni les mettre à la disposition du public sans établir de mécanisme de contrôle précis. La *Loi sur l'accès à l'information et la protection de la vie privée* du Manitoba est un exemple du

type de contrôle auquel nous pensons : cette loi interdit explicitement la communication en vrac ou en grande quantité des renseignements personnels versés dans un registre. La *LPRP* fédérale devrait comprendre une telle disposition, parmi d'autres sur les registres gouvernementaux.

Élargir le mandat du Commissaire à la protection de la vie privée
La capacité du Commissaire à la protection de la vie privée de remplir son rôle d'ombudsman a souvent été limitée par les restrictions imposées par la *LPRP*. Par exemple, le rôle du Commissaire en tant que défenseur du droit à la vie privée a souffert du peu de recours juridiques que lui accorde la Loi. Comme nous l'expliquions plus haut, le Commissaire ne peut à l'heure actuelle porter devant les tribunaux que les refus d'accès aux renseignements personnels. La Loi reste muette quant à un recours juridique sur la collecte, l'usage, la communication et la destruction des renseignements personnels sur les Canadiens effectués par le gouvernement de façon inappropriée. La Loi n'exige pas non plus du Commissaire que son personnel étudie et documente certains enjeux pour la vie privée, non plus qu'il étudie les impacts de nouvelles lois et de nouveaux systèmes informatiques sur la vie privée. Le Commissaire n'est pas non plus mandaté par la Loi pour éduquer le public sur son droit à la vie privée. Même si ces lacunes dans la Loi n'empêchent le Commissaire à la protection de la vie privée d'en repousser les limites lorsque le droit à la vie privée est menacé, l'absence de ce mandat signifie un manque d'argent dont les conséquences restreignent le travail de l'ombudsman de la vie privée du public. La Loi doit donc faire clairement état de ces activités.

Voilà quelques-unes des principales recommandations que nous demanderons au Parlement d'examiner afin de modifier la *LPRP* actuelle. Par le passé, nous avons tenté de préciser certaines dispositions. Aujourd'hui, cependant, la Loi a besoin de rien de moins qu'une révision majeure. Avec l'adoption de la Loi C-6, la modification de la *LPRP* devient un impératif législatif. Il est rare qu'on ait l'occasion de réviser et de restructurer une loi ; il est d'autant plus important de saisir l'occasion et de faire le nécessaire pour protéger les intérêts des générations futures face à leur vie privée.

L'avenir du recensement

Le recensement de 2001 — une collecte plus claire

C'est le 15 mai 2001 que Statistique Canada demandera à quelque 31 millions de Canadiens, répartis dans près de 12,8 millions de foyers, de remplir leur formulaire de recensement. Quelque 40 000 travailleurs sur le terrain travailleront à ce projet à partir de cinq bureaux régionaux, et le coût total du projet s'élèvera à 400 millions de dollars.

Chaque recensement constitue la plus imposante collecte de renseignements personnels par le gouvernement fédéral, et la plus poussée pour le cinquième des Canadiens à qui Statistique Canada demande de remplir un questionnaire détaillé. Il va sans dire que ce projet soulève l'intérêt du Commissaire fédéral à la protection de la vie privée.

Comme dans le cas des recensements antérieurs, 80 p. 100 des foyers canadiens recevront un questionnaire abrégé demandant des données démographiques élémentaires telle la date de naissance, le sexe, l'état civil et les liens entre les personnes résidant à cette adresse. En outre, une question quant à la première langue apprise à la maison pourrait y être ajoutée.

Le cinquième restant de la population recevra un questionnaire détaillé. En 1996, ce questionnaire posait (en plus des questions démographiques élémentaires précédentes) quelque 47 autres questions portant sur les handicaps physiques, les connaissances linguistiques, le niveau de scolarisation, le travail, les tâches ménagères, le pays et l'ethnie d'origine, le statut autochtone, le logement, les coûts d'hébergement et le revenu.

Bien que Statistique Canada renseigne généralement bien les Canadiens sur la façon de remplir et d'expédier leur questionnaire de recensement, il en va différemment sur le fait que les préposés locaux au recensement vérifient ces questionnaires une fois remplis avant de les faire suivre au siège social de

Statistique Canada à Ottawa. Les Canadiens ne savent donc pas que leurs réponses peuvent être lues par une personne dont ils sont connus.

De toutes les plaintes concernant la vie privée reçues par le Commissariat suite aux recensements de 1991 et de 1996, celles qui ont suscité les protestations les plus véhémentes découlaient des situations où les préposés au recensement connaissaient les personnes dont ils traitaient le questionnaire. Dans la plupart des cas, les plaignants étaient furieux et vexés d'apprendre que c'était des voisins, préposés au recensement, qui avaient révisé leur questionnaire au lieu d'un quelconque fonctionnaire d'Ottawa.

Les plaignants se sont sentis trahis et outragés lorsqu'ils ont appris que des renseignements personnels et de nature délicate fournis à Statistique Canada étaient révisés localement par un ami, un voisin ou un parent travaillant à mi-temps pour le bureau de recensement. Que des renseignements sur leur revenu, leurs versements hypothécaires, leurs épargnes ou leurs factures d'électricité soient ainsi accessibles allaient à l'encontre de la promesse de confidentialité que ces gens avaient reçue.

La grande majorité des plaignants se disait peu réconfortée par le serment de secret prêté par les préposés au recensement et les amendes ou peines d'emprisonnement résultant d'une divulgation de renseignements personnels. Ces deux mesures n'atténuaient que trop peu leur gêne et l'atteinte à leur vie privée. Si leurs questionnaires avaient été révisés par un parfait inconnu de Statistique Canada à Ottawa, ces gens auraient éprouvé une atteinte moindre. Selon le Commissaire à la protection de la vie privée, cette collecte de renseignements par des voisins connus démontre un manque total de compréhension de ce que constitue la vie privée.

Afin de contourner cette problématique, Statistique Canada a avisé le Commissaire de son intention de remplacer l'actuel système par un processus centralisé de révision. Tous les questionnaires du recensement seraient acheminés aux bureaux de district pour y être traités plutôt que renvoyés aux préposés locaux. Ces derniers se limiteraient au suivi de réponses manquantes ou à la clarification de détails que le bureau de district ne pourrait obtenir par téléphone. Statistique Canada serait alors à même de s'assurer que ces préposés ne sont pas de l'endroit.

Ce nouveau processus centralisé a été mis à l'épreuve lors du recensement de 1996 et du test national d'octobre 1998 préalable au recensement de 2001. Cependant, Statistique Canada n'a malheureusement pas obtenu les résultats escomptés, le nouveau processus permettant à quelqu'un de ne pas remplir son questionnaire, de ne le remplir qu'en partie ou de ne pas le renvoyer à

Statistique Canada, amenant ainsi davantage de contacts (et donc de risques d'atteinte à la vie privée) de la part des préposés au recensement que l'ancienne méthode. Le nouveau processus ne sera donc pas utilisé pour le recensement de 2001, une décision renforcée par les erreurs et oublis notés dans la liste nationale d'adresses résidentielles détenue par Statistique Canada.

Statistique Canada continue d'étudier d'autres options comme le recours à des entrevues téléphoniques avec aide informatique dans deux bureaux régionaux ou à l'Internet. Cette dernière solution serait d'ailleurs mise à l'essai sur deux sites Web dans le cadre du prochain recensement. Les répondants se verraient octroyer un numéro d'identification personnel et leurs réponses seraient chiffrées, éliminant de ce fait le risque qu'un questionnaire ne se retrouve dans les mains d'un préposé local. Statistique Canada se penche également sur la possibilité de réduire le nombre de communications entre les préposés et les personnes recensées. L'organisme vise en fait une baisse du taux de rejet des questionnaires détaillés (formulaire 2B) de 55 à 39 p. 100, ce qui permettrait de réduire considérablement le nombre de contacts avec les ménages et les heurts pouvant en découler.

On procédera à deux tests comparés au cours du prochain recensement. Le premier verra l'envoi de quelque 125 000 questionnaires détaillés (soit environ 5 p. 100 de tous ceux-ci) pour lequel aucun suivi ni révision ne seront effectués. Le second visera un échantillon de 325 000 de ces mêmes questionnaires (environ 14 p. 100) n'impliquant qu'un suivi téléphonique.

De plus, Statistique Canada affectera ses préposés des régions urbaines à des quartiers ou ils sont inconnus des habitants, réduisant de ce fait le risque de collecte de renseignements de personnes de leur entourage. Ce critère en sera un d'embauche dans le cadre du prochain recensement. En région rurale et dans les petits villages, cependant, il ne sera pas toujours possible de satisfaire à ce critère du fait du nombre plus limité de candidats disponibles. En outre, Statistique Canada croit que la seule manière de s'assurer que tous les ménages sont recensés en région rurale est d'y affecter un personnel connaissant la région.

Cependant, afin d'atténuer le problème, un message paraîtra tant sur le questionnaire que sur l'enveloppe de retour informant les gens que leurs questionnaires seront révisés localement par un représentant de Statistique Canada. Les personnes opposées à cette pratique apprendraient des préposés

locaux ou téléphoniques au recensement qu'elles peuvent faire parvenir leurs questionnaires à un commissaire au recensement ou au bureau régional. Statistique Canada fournira également à ses préposés une formation et des mécanismes supplémentaires portant sur l'importance de protéger les renseignements qu'ils recueilleront lors du recensement, et les sensibilisant davantage aux questions de protection de la vie privée.

Le problème reste toutefois entier, même si ces mesures en résoudront certains aspects. Le Commissariat est préoccupé du manque de clarté du processus. À titre d'exemple, le message suggéré pour l'endos des enveloppes à l'effet qu'un préposé réviserait les questionnaires ne mentionne nullement la possibilité que ce préposé soit connu des personnes ayant rempli ces questionnaires.

Puisque Statistique Canada reconnaît qu'il n'est pas inhabituel que les habitants d'un endroit donné connaissent le préposé au recensement (surtout en milieu rural), ces habitants doivent non seulement être clairement prévenus de la possibilité précédente mais également avoir d'autres possibilités de renvoi de leurs questionnaires. Ceci s'applique tant aux questionnaires détaillés qu'aux questionnaires abrégés, ces derniers posant en effet une question sur les relations entre personnes du même sexe. Dans cette optique de clarté, le Commissariat à la protection de la vie privée a suggéré le libellé suivant pour le guide explicatif et les deux questionnaires du recensement :

> « Bien que Statistique Canada tente de s'assurer que ses préposés au recensement travaillent à proximité de leur lieu de résidence tout en ne connaissant pas les personnes recensées dans leur secteur de travail, il est possible que certaines personnes connaissent leur préposé. Si tel est votre cas et que vous ne vous sentez pas à l'aise à l'idée de communiquer vos renseignements personnels à ce préposé, veuillez appeler sans frais notre Ligne d'aide au recensement pour apprendre les autres façons que vous avez de nous faire parvenir votre questionnaire (une fois rempli) sans passer par votre préposé. »

Le Commissariat à la protection de la vie privée croit aussi que le problème pourrait être en partie évité si chaque préposé était obligé de mentionner ces autres façons à toute personne connue. Un tel avis dès le contact initial est préférable à une protestation. Les préposés devraient également être obligés de remettre au commissaire régional au recensement le questionnaire rempli de toute personne connue sans l'avoir lu.

Données de recensements antérieurs

L'année dernière, nous avons fait un rapport sur le débat entourant la publication des résultats de recensements effectués après 1901. Tous les recensements effectués au Canada depuis 1901 ont été l'objet de la promesse réitérée, d'abord dans la réglementation, puis dans la législation, de ne divulguer aucun résultat individuel à l'extérieur de Statistique Canada. La loi interdit donc à Statistique Canada de communiquer les résultats de recensements aux Archives nationales. Irrités, les historiens et les généalogistes qui cherchaient un moyen d'accéder à l'information ont demandé publiquement que des changements rétroactifs soient apportés à la loi.

Toute promesse du gouvernement d'assurer la confidentialité doit être prise au sérieux, et la promesse de protéger les données du recensement est particulièrement importante. Les réponses aux questions du recensement sont des renseignements personnels. Au cours du 20e siècle, les questions du recensement sont devenues de plus en plus indiscrètes ; même au début des années 1900, certaines questions à propos notamment des études, de la religion, de la nationalité, de la race, de la profession et des revenus étaient déjà gênantes. Les réponses révélaient de l'information que les intéressés n'auraient pas nécessairement accepté de rendre publique. Les Canadiens sont tenus de répondre aux questions des recensements, et les peines maximums encourues pour manquer à ce devoir sont sévères : des amendes ou l'emprisonnement. S'assurer que l'information demeure confidentielle, s'en servir uniquement à des fins statistiques et ne pas la communiquer sous une forme reconnaissable sont sans doute les compromis qui ont incité le public à accepter les recensements et à se conformer à la loi.

Malgré l'interdiction indiscutable de communiquer les réponses aux questions du recensement, le ministre de l'Industrie a demandé l'an dernier à Statistique Canada de songer à des façons de modifier la loi pour permettre l'accès aux réponses individuelles. Statistique Canada a proposé deux options : modifier la *Loi sur la statistique* pour permettre d'accéder aux résultats du recensement de 2001 et de tous les recensements subséquents ; ou modifier rétroactivement la *Loi sur la statistique* pour outrepasser les dispositions relatives à la confidentialité des résultats. Le Commissaire à la protection de la vie privée s'est opposé aux deux options parce que dans le premier cas, l'absence d'une garantie de confidentialité risquerait de compromettre le processus de recensement et dans le second cas, la promesse juridique faite par le Parlement aux Canadiens serait rompue.

En guise de réponse, le ministre a créé un comité d'experts pour examiner les problèmes et faire des recommandations. Le Commissaire a comparu devant ses membres en février 2000.

Il a fortement encouragé ces derniers à reconnaître les grandes questions sociales concernant la vie privée et la gestion publique qui sous-tendent le débat. Il leur a fait remarquer que la question n'était pas de savoir si un intérêt « personnel » ou « individuel » ayant trait à la vie privée devrait céder le pas à un intérêt « public » ou « sociétal » lié à la recherche généalogique et historique. Les historiens et les généalogistes qui veulent accéder aux résultats du recensement ne peuvent pas prétendre être les seuls à représenter l'intérêt public ou à exprimer un droit public. En effet, la vie privée est, elle aussi, un droit public qui est à la base des libertés et du respect mutuel essentiels à la société canadienne. Le comité n'était pas simplement appelé à prendre une décision sur la vie privée des personnes recensées de 1906 ou de 1911. Sa décision, laquelle influera certes sur la vie privée de ces personnes, aura des répercussions également sur celle de tous les Canadiens.

Un bon nombre de questions fondamentales sur la vie privée sont remises en jeu. La plus importante d'entre elles est le principe énoncé dans toutes les lois et les codes sur la protection de l'information, selon lequel un renseignement personnel ne doit pas servir à des fins autres que celles pour lesquelles il a été recueilli. Tout autre usage ne devrait se faire qu'avec le consentement de la personne qui a donné ce renseignement.

Il est également difficile de conserver des renseignements personnels plus longtemps que la période prévue ou déclarée. L'existence même de ces dossiers, longtemps après qu'ils ont rempli leur rôle statistique légitime, ouvre la porte à des utilisations sans aucun rapport avec les fins pour lesquelles les résultats du recensement ont été recueillis. Selon les défenseurs de la vie privée, voilà un exemple typique de détournement de finalités qui rappelle l'importance d'établir et de respecter des limites quant à la période de conservation de l'information.

Finalement, il faudrait savoir à quel moment on peut considérer que cessent les droits d'une personne à la protection de sa vie privée. Aux dires de certaines personnes, les droits des personnes recensées en 1906 et 1911 n'existeraient plus : même en supposant que toutes ces personnes sont décédées (ce qui n'est pas obligatoirement le cas), la proposition ne va pas de soi. En règle générale, la société reconnaît que certains droits subsistent après le décès de quelqu'un ; c'est sur ce principe que les gens s'appuient pour dicter dans leur testament la répartition de leurs biens après leur décès, et ils sont même encouragés à le faire. Les dispositions de la *Loi sur la protection des*

renseignements personnels prévoient d'ailleurs que les renseignements d'un individu demeurent « personnels » 20 ans après le décès de l'intéressé.

Le Commissaire a fait ressortir aux membres du comité que toute proposition visant à modifier la loi rétroactivement devrait être envisagée avec une grande prudence, de crainte que le résultat n'atténue la confiance à l'égard des promesses d'organismes gouvernementaux ou même de gouvernements se targuant de diriger leurs électeurs avec le consentement de ces derniers. Les tenants d'une modification rétroactive la présentent comme inoffensive et décrivent la promesse de confidentialité comme « une formalité juridique dans une loi désuète ». Cependant, le Commissaire a rappelé au comité que cette promesse de confidentialité est essentielle à l'obtention de réponses aux questions du recensement.

Les Canadiens n'ont jamais été particulièrement à l'aise avec les questions indiscrètes du recensement. Le nombre de demandes et de plaintes qui ont été adressées au Commissariat à la protection de la vie privée au cours des années en sont un indice. Pourtant, le taux de réponse au recensement canadien est élevé. Malgré l'indiscrétion des questions, le caractère délicat des réponses et la gêne causée par le processus, les Canadiens consentent à y prendre part.

En partie, la raison est qu'ils y sont contraints, le refus de répondre à une question indiscrète ayant toujours été puni d'une amende ou d'une peine d'emprisonnement. Cependant, le gouvernement du Canada ne s'appuie pas principalement sur ces mesures coercitives. En effet, comme des générations d'écoliers canadiens s'en sont rendus compte, la société canadienne s'enorgueillit d'avoir un gouvernement responsable qui dirige avec le consentement de la population. Ce n'était pas la menace de l'utilisation de la force qui était au centre du processus de recensement, mais bien une entente entre le gouvernement et les Canadiens, selon laquelle ces derniers répondraient à des questions gênantes mais verraient leurs réponses protégées. L'abolition rétroactive de la promesse de confidentialité risque de banaliser cette entente parmi d'autres.

Par ailleurs, le Commissaire à la protection de la vie privée a recommandé aux membres du comité de songer au moins à un compromis pour atténuer l'incidence sur la vie privée et la gestion publique s'ils choisissaient de ne pas appuyer les promesses du gouvernement et les droits liés à la protection des renseignements personnels des Canadiens. Reconnaissant l'intérêt particulier que présentent les résultats des recensements — l'une des rares sources documentaires sur la population canadienne du début du 20e siècle — pour les historiens et les généalogistes, le Commissaire a proposé de choisir une

date à partir de laquelle les objectifs des historiens et des généalogistes pourraient être réalisés sans avoir accès à ces résultats. Les données des recensements préalables à la date limite pourraient être communiquées aux Archives nationales, tandis que tous les résultats des recensements postérieurs à cette date seraient détruits après avoir rempli leur rôle statistique légitime.

Le Commissaire a fortement recommandé au comité de songer à retirer les données de base (noms, âges, adresses) des résultats détaillés, en se fondant sur le principe que le gouvernement devrait d'abord tenter de mettre en pratique la mesure la moins envahissante pour atteindre ses objectifs et ne recourir aux mesures plus gênantes que si elles sont réellement nécessaires.

Si le Parlement supprime la disposition sur la confidentialité de la *Loi sur la statistique*, le processus doit être clair. Statistique Canada doit informer les Canadiens au moment du recensement que leurs renseignements seront éventuellement publiés. Si, comme l'indique Statistique Canada, la confidentialité compte parmi les moyens les plus efficaces pour s'assurer de la collaboration des Canadiens, le Parlement doit alors trouver un autre moyen pour convaincre la population de se prêter à cet exercice. Le Commissaire a également vivement conseillé au comité d'examiner le modèle australien, qui permettra aux personnes recensées en 2001 de choisir de mettre ou non de côté leurs résultats et d'en autoriser la publication 99 ans plus tard (à l'heure actuelle, l'Australie détruit les résultats des recensements).

Finalement, le Commissaire signale que la modification rétroactive de l'entente entre les Canadiens et le gouvernement annule les conditions qui sous-tendaient la participation des Canadiens au recensement. Une telle modification doit être l'objet d'un débat parlementaire approfondi auquel participeront tous les députés qui devront répondre publiquement de leurs actes. L'exposé du Commissaire, intitulé *Les résultats de recensement, la protection de la vie privée et les questions de gestion publique*, est disponible à nos locaux ou par le biais de notre site Web.

Le point sur le numéro d'assurance sociale

Certaines questions reviennent toujours. Lorsqu'on regarde les rapports annuels antérieurs, on constate que le numéro d'assurance sociale (NAS) a toujours fait couler beaucoup d'encre. Le rapport de cette année respecte cette tradition : deux articles portent sur le sujet. Le premier a trait aux propositions d'amélioration de la gestion du NAS du ministère du Développement des ressources humaines Canada (DRHC), suite au rapport de l'examen du Vérificateur général. Ce rapport, traité dans notre dernier rapport annuel, soulevait plusieurs inquiétudes dont l'utilisation de plus en plus répandue du NAS pour identifier les gens. Au nombre des efforts déployés en vue de contrôler l'utilisation de ce numéro, nous retrouvons plusieurs projets de lois privés, tel celui en 1979 du député Perrin Beatty. Puis en 1987, un comité parlementaire proposait la mise en place de contrôles stricts suite à un examen approfondi de trois ans de la *Loi sur la protection des renseignements personnels*. Ces deux initiatives sont cependant restées lettre morte bien que le gouvernement ait imposé une politique limitant l'utilisation du NAS au sein du gouvernement. Aujourd'hui, vingt ans après les restrictions proposées par Perrin Beatty, le gouvernement n'a toujours pas arrêté les façons de contrôler l'utilisation du NAS dans le secteur privé. Le temps est au geste, non plus à la parole.

Le deuxième article traite d'un projet pilote mené au Nouveau-Brunswick, et dont l'objectif est d'améliorer l'administration du NAS, un autre enjeu de longue date, en accélérant l'émission des NAS et en améliorant le processus de vérification des renseignements requis pour son obtention.

Exposé de principe de DRHC

L'une des conséquences de l'examen du Vérificateur général a vu le Comité permanent de la Chambre des communes sur les droits de la personne et la condition des personnes handicapées chargé d'étudier divers aspects du régime administratif et stratégique qui régit le NAS. Le rapport du Comité permanent, intitulé *Au-delà des chiffres : L'avenir du numéro d'assurance sociale au*

Canada, recommandait une loi pour établir les usages licites du NAS et les pénalités imposées pour son usage détourné. Il suggérait également que DRHC prépare un exposé sur les options possibles permettant de régler les problèmes administratifs de longue date ayant trait à la gestion du NAS et aux préoccupations relatives à la vie privée.

En décembre 1999, DRHC déposait devant le Parlement son exposé de principes sur la question. Le document traite de trois options stratégiques : 1) transformer le NAS en numéro national d'identification de la clientèle soutenu par la technologie biométrique ; 2) effectuer des réformes administratives pour améliorer l'administration du NAS dans le contexte d'une loi limitant explicitement les usages et les utilisateurs du NAS ; et 3) apporter des réformes administratives pour améliorer l'administration du NAS dans le contexte d'un cadre législatif légèrement modifié auquel se rajouteront les mécanismes de protection contre l'abus de renseignements tels le NAS dans le secteur privé que prévoit la Loi C-6.

L'exposé de principes rejetait l'option qui consiste à transformer le NAS en un numéro national d'identification de la clientèle, notamment à cause des coûts prohibitifs associés à la mise en place d'un système soutenu par la technologie biométrique — le gouvernement a estimé qu'il en coûterait de 1,1 milliard à 3,6 milliards de dollars pour émettre aux Canadiens des cartes à la fine pointe de la technologie. De plus, l'établissement d'un tel système national d'identification entraînerait de graves problèmes au chapitre de la vie privée. Pourtant, l'exposé de principes a également rejeté la possibilité d'imposer des restrictions législatives à l'utilisation du NAS, ignorant ainsi l'une des recommandations clés du Comité permanent. Selon DRHC, de telles restrictions mèneraient presque tout droit à l'augmentation des coûts d'exploitation des entreprises, qui seraient obligées de se reposer sur un système de vérification du crédit généralement moins fiable.

L'exposé de principes laisse croire que, à l'exception de certaines modifications limitées apportées à la *Loi sur l'assurance emploi*, les problèmes d'administration du NAS pourraient être résolus dans le cadre législatif et stratégique actuel, et que les préoccupations de longue date en ce qui a trait à l'utilisation et aux abus non contrôlés du NAS dans le secteur privé seraient réglées, dans une large mesure, par l'adoption de la Loi C-6. Parmi les mesures administratives que l'on compte prendre pour améliorer l'administration du NAS, mentionnons la réduction du nombre de documents acceptés comme preuves d'identité pour les demandeurs de nouveaux NAS et l'augmentation de l'accès aux sources de documents — comme les registres provinciaux de l'état civil — à des fins de vérification.

Dans le but de détecter et de décourager l'utilisation du NAS à des fins frauduleuses, l'exposé de principes cite également des mesures qui ont été prises pour élargir l'accès des utilisateurs au Registre d'assurance sociale (RAS). Cela permettrait à certaines administrations provinciales, et peut-être même à des organismes du secteur privé qui emploient le NAS, de vérifier l'authenticité du NAS et l'identité de la personne qui déclare en être le titulaire authentique. En plus de pouvoir accéder aux renseignements de base qui permettent d'identifier une personne, les utilisateurs auraient également accès à certaines informations sur la situation du NAS. Par exemple, que le compte appartient à une personne décédée, qu'il a été annulé, qu'il est inactif depuis cinq ans ou qu'il fait l'objet d'une enquête. L'accès à de tels renseignements permettrait aux utilisateurs de remarquer des anomalies ou des problèmes possibles associés au numéro.

Dans le même but, l'exposé de principes recommande d'apporter certaines modifications à la *Loi sur l'assurance emploi* qui permettraient d'élargir le nombre des infractions liées au NAS étant sujettes à des sanctions administratives dont la sévérité serait augmentée. Parmi les infractions que l'on se propose de sanctionner, mentionnons 1) l'utilisation illicite du NAS dans une demande de prestations d'assurance emploi, 2) l'utilisation illicite du NAS auprès d'une autre administration fédérale, provinciale ou municipale, et 3) l'utilisation illicite d'un NAS dans le cadre d'une transaction avec le secteur privé. Les pénalités imposées à ces diverses infractions se situeraient entre 400 $ et 1 200 $.

Même si nous sommes heureux que le gouvernement ait rejeté la proposition de mettre sur pied un système national d'identification des citoyens, une idée à laquelle nous nous opposons depuis longtemps, nous avons été déçus du refus du gouvernement de suivre la recommandation du Comité permanent et de légiférer quant à l'usage et aux utilisateurs du NAS. Selon nous, un régime législatif permettant aux gouvernements fédéral et provinciaux d'utiliser le NAS à n'importe quelle fin et l'élargissement du droit d'accès au RAS à des fins d'identification de la clientèle risquent de transformer d'office le NAS en ce que le gouvernement a pourtant déclaré qu'il ne devait pas devenir, soit un numéro national d'identification de la clientèle.

De plus, même si nous pouvons en principe comprendre la raison pour laquelle DRHC recueillerait et conserverait certains renseignements sur le statut d'un NAS ainsi que le bien-fondé du partage de tels renseignements avec les utilisateurs autorisés du NAS, l'initiative présente des risques importants pour la vie privée si elle n'est pas strictement réglementée. À l'heure actuelle, le RAS recueille et communique peu de renseignements, mais l'exposé de principes du gouvernement ouvre la voie à l'expansion.

Les risques que pose l'actuel régime législatif permissif justifient davantage l'adoption d'une loi propre au NAS. DRHC a cependant rejeté cette option principalement parce qu'il croit que le fait de restreindre la collecte et l'usage du NAS par le secteur privé imposerait à ce dernier un préjudice financier et des risques indus. Le ministère compte se rabattre sur la Loi C-6 pour contrôler tout abus du NAS par les entreprises privées.

La notion d'un préjudice financier ne repose selon nous sur aucun fondement : DRHC s'était engagé à interroger les entreprises privées sur leur utilisation légitime et abusive du NAS, mais a préparé son exposé de principes sans l'avoir fait. Ce sondage, préparé en collaboration avec Statistique Canada, devrait débuter sous peu.

Nous espérons que ce sondage nous en apprendra davantage quant aux capacités de la Loi C-6 d'empêcher ou de régler tous les abus du NAS qui ont actuellement cours dans le secteur privé. Même si le projet de loi exige des entreprises privées qu'elles obtiennent notre consentement avant d'utiliser notre NAS, il reste que ce dernier sera utilisé à des fins pour lesquelles il n'a jamais été conçu. Le fait de permettre que le secteur privé s'en tire à bon compte au mépris de la protection juridique légitime qui entoure le numéro identifiant chaque Canadien(ne) dans les programmes sociaux et auprès du fisc revient à mettre la charrue devant les bœufs.

"VU LE MAUVAIS ÉTAT DE VOS SIGNES VITAUX FINANCIERS, JE CRAINS DE NE PAS POUVOIR VOUS OPÉRER."

Le risque de couplages secrets de données augmentera substantiellement si différentes entreprises privées utilisent le NAS comme numéro de dossier. Ce dernier, en effet, peut au même titre que d'autres numéros de compte servir de clé d'accès permettant l'échange ou le couplage de renseignements. Ce risque prend toute son importance face au principe du « consentement tacite » qui est explicitement reconnu par la Loi C-6. D'autres lois étrangères relatives à la protection des données personnelles — dont celles de Hong Kong, de l'Australie et de la Nouvelle-Zélande — limitent explicitement le droit des entreprises privées d'utiliser les numéros de dossier ou d'identification que d'autres organismes ont assignés. Comme la Loi C-6

ne comprend aucune interdiction de ce genre, il est nécessaire d'instaurer des restrictions législatives spécifiques au NAS.

Bien que nous félicitions DRHC de vouloir élargir la liste des infractions sujettes à des sanctions administratives, nous doutons du fait que ces sanctions suffiraient à décourager de telles infractions. Le vol d'identité est une entreprise criminelle de plus en plus rentable et répandue et il y a gros à gagner de l'abus du NAS et d'autres numéros d'identification. Selon nous, les pénalités imposées pour l'abus du NAS devraient être proportionnelles aux problèmes qu'affronteraient les victimes innocentes d'un tel abus. Les propositions actuelles à ce sujet sont encore loin du compte.

Projet pilote au Nouveau-Brunswick

Le projet pilote mené d'avril à octobre 1998 au Nouveau-Brunswick fait l'objet d'un partenariat entre DRHC et la direction générale de l'état civil du Nouveau-Brunswick. Pendant cette période, les natifs de la province pouvaient présenter une demande de NAS par téléphone par l'entremise d'un Système intégré de réponse vocale et d'un agent de DRHC. Ensuite, le ministère fédéral vérifiait en ligne l'identité du requérant grâce aux registres provinciaux des naissances, des mariages, des changements de nom et des décès. Une fois l'information vérifiée, l'agent de DRHC pouvait approuver la demande, créer une nouvelle entrée dans le RAS et émettre un nouveau NAS au requérant par téléphone. La carte d'assurance sociale suivait dans les cinq à sept jours.

Au début de septembre 1999, DRHC a présenté son rapport d'évaluation du projet pilote au Commissariat à la protection de la vie privée pour commentaire. Nous avons évalué si le fait d'utiliser les données provinciales de l'état civil pour valider l'information sur les requérants d'un NAS était conforme aux principes équitables de l'information prévus dans la *Loi sur la protection des renseignements personnels*. Essentiellement, ces principes définissent comment et quand recueillir, conserver, utiliser, divulguer à des tiers et détruire des renseignements personnels.

L'examen a conclu que la *Loi sur l'assurance emploi* et la *Loi sur le Régime de pensions du Canada* conféraient à DRHC l'autorisation légale de recueillir tous les renseignements nécessaires pour identifier avec exactitude les personnes qui présentent une demande de NAS, de remplacement d'une carte d'assurance sociale ou de modification de leur dossier qui figure dans le registre d'assurance sociale. Nous avons également déterminé que la *Loi sur les statistiques de l'état civil* du Nouveau-Brunswick permettait à DRHC d'accéder à certains renseignements personnels afin de donner un NAS aux personnes nées au Nouveau-Brunswick et de s'assurer que les

renseignements fournis par les requérants étaient exacts.

Les données accessibles à DRHC se limitaient aux naissances, mariages, décès et changements de nom, éléments nécessaires pour vérifier l'identité d'un requérant au téléphone. Même si le fait de recueillir ces renseignements semblait directement relié et nécessaire à l'exécution d'un programme légitime de DRHC, nous avions des réserves quant à la collecte de renseignements provenant du registre des mariages de la province. À notre avis, DRHC peut utiliser des renseignements sur l'état matrimonial pour authentifier l'identité d'un requérant d'un NAS, mais ceux-ci ne devraient être enregistrés dans la base de données du RAS que si le requérant a changé de nom suite à un mariage.

DRHC a également signalé que plus de 500 demandes de NAS avaient été rejetées pour diverses raisons au cours du projet pilote. Le Commissariat aimerait savoir ce qu'il est advenu des renseignements (dont les numéros du certificat de naissance et de la carte de crédit) fournis par les requérants ayant changé d'idée en cours d'appel ou ayant vu leur demande refusée : DRHC a-t-il conservé les renseignements ?

Le Commissariat a également examiné la transparence du processus pour les requérants. Nous avons découvert que le système leur fournissait des directives claires sur la façon de présenter une demande de carte. On les informait des renseignements requis, de la façon dont ils seraient utilisés et qui y aurait accès. Les requérants pouvaient raccrocher à n'importe quel moment. En restant en ligne et en fournissant les renseignements demandés par le biais du clavier du téléphone, les requérants autorisaient DRHC à traiter leur demande. Nous croyons cependant que DRHC devrait préciser aux requérants qu'ils donnent leur consentement lorsqu'ils fournissent les renseignements demandés.

Même si les données de l'état civil peuvent constituer une source précieuse pour la vérification des données du système d'enregistrement des NAS, le fait d'y avoir recours pourrait nuire à la vie privée. Les dossiers de naissance, de mariage et de décès ont de tout temps servi à émettre des certificats de naissance, de mariage et de décès et à compiler des statistiques. Toute divulgation de ces renseignements à des fins administratives autres que celles précisées au moment de la collecte des renseignements pourrait violer les codes provinciaux de pratiques équitables de traitement de l'information. Ces derniers, au même titre que la *Loi sur la protection des renseignements personnels*, exigent que les renseignements personnels ne soient utilisés qu'aux fins pour lesquelles ils ont été obtenus. Toute dérogation à ces principes doit être justifiée par de solides raisons d'intérêt public.

Si DRHC veut étendre son projet à d'autres provinces et territoires, les organismes provinciaux responsables de l'état civil devront répondre à cette question. Ils devront aussi déterminer s'ils ont le cadre législatif nécessaire pour permettre à DRHC d'accéder en ligne aux registres de l'état civil aux fins de son programme d'enregistrement du NAS.

Outre, les considérations juridiques et relatives à la vie privée, le couplage des données de l'état civil entre les organismes provinciaux et territoriaux responsables et DRHC soulève des inquiétudes quant à la confidentialité et à la sécurité des données. Les organismes qui effectuent des couplages de données doivent disposer de tous les mécanismes de protection nécessaires pour s'assurer que les données couplées ne sont accessibles qu'aux bonnes personnes au bon moment et pour la bonne raison. Donc, la confidentialité et la sécurité des données sur l'état civil et les problèmes de connectivité et de compatibilité entre les divers systèmes d'exploitation seront des problèmes à régler si DRHC décide d'étendre son projet pilote aux autres provinces et territoires. Dans le cas du Nouveau-Brunswick, même s'il nous manque certains détails techniques, il semble que le système était doté des mesures de contrôle nécessaires pour assurer la confidentialité et la sécurité de tous les renseignements échangés.

Une fois le projet pilote terminé, le 2 octobre 1998, la direction de l'état civil du Nouveau-Brunswick a accepté que tous ses renseignements nécessaires au traitement d'une demande de NAS soient enregistrés dans les serveurs de DRHC. Le Commissariat à la protection de la vie privée voit là deux manquements sérieux. Dans un premier temps, en recueillant d'avance de l'information sur des personnes qui n'ont pas encore présenté de demande ou qui pourraient ne jamais en présenter, DRHC recueille plus de renseignements qu'il n'est nécessaire, violant ainsi les limites sur la collecte qu'impose la *Loi sur la protection des renseignements personnels*. De plus, cette façon de faire ne respecte pas l'un des principes fondamentaux de la vie privée, le consentement, qui exige qu'une institution fédérale, dans la mesure du possible, obtienne la permission de la personne concernée avant de recueillir ses renseignements auprès d'une autre source.

Nous avons également appris que DRHC continue d'accéder aux registres de l'état civil du Nouveau-Brunswick lorsqu'elle traite les demandes écrites de NAS provenant de natifs de la province. Nous ignorons si ces requérants ont été clairement prévenus du fait que les renseignements qu'ils soumettent dans leur demande seront comparés à ceux de l'état civil de leur province. DRHC a la responsabilité d'informer ces gens de l'usage prévu de leurs données. Ne pas communiquer cette information avant que la personne fournisse les renseignements demandés va à l'encontre des grands principes de protection

de la vie privée.

Nous avons fait parvenir au Comité permanent nos commentaires sur le rapport d'évaluation au début de décembre 1999. Nous avons par la suite rencontré les représentants de DRHC vers la fin février 2000.

À la suite de cette rencontre, DRHC s'est engagé à informer le public que le RAS contiendrait tous les noms utilisés antérieurement (tel le nom d'un ancien mari). Ils ont aussi accepté d'étudier la notion que l'entente survenue entre DRHC et le gouvernement du Nouveau-Brunswick relative au stockage de toutes les données provinciales de l'état civil sur un serveur du ministère fédéral conserve à la province son titre de propriétaire des renseignements et stipule clairement que ces derniers ne serviront qu'à traiter des demandes de NAS. DRHC a accepté de modifier les avis imprimés sur les formulaires et lus au téléphone pour y indiquer les usages que le ministère fait des renseignements de l'état civil provincial.

Les responsables de DRHC nous ont expliqué que les renseignements concernant une demande téléphonique rejetée étaient détruits. Quant aux demandes écrites, les renseignements sont conservés dans un dossier séparé pendant six mois dans l'attente d'une seconde demande du requérant. DRHC se penchera sur une façon de prévenir les requérants que leurs renseignements, qu'ils soient fournis par écrit ou par téléphone, seront conservés pendant six mois afin de servir au traitement de toute nouvelle demande ultérieure.

Pour terminer, DRHC a promis de tenir le Commissariat au courant de tout effort menant à l'implantation de son projet de demande téléphonique de NAS partout au pays.

Le dossier unique sur chaque citoyen existe… à DRHC

La vérification

Il y a deux ans, le Commissariat à la protection de la vie privée a décidé de concentrer la totalité de ses maigres effectifs (quatre personnes) de vérification sur Développement des ressources humaines Canada (DRHC). Pourquoi ?

Notre décision allait de soi. La réorganisation du gouvernement fédéral avait fait de DRHC un monstre virtuel, dont les ordinateurs renferment la plus grande quantité de renseignements personnels sur les Canadien(ne)s de tout l'appareil fédéral. Le ministère a en effet hérité des programmes de main-d'œuvre de l'ancien ministère du Travail, des activités de sécurité sociale et du revenu de l'ancien ministère de la Santé et du Bien-être, des services de développement social et d'éducation de l'ancien Secrétariat d'état, et de l'assurance-chômage et des programmes d'emploi de l'ancien ministère de l'Emploi et de l'Immigration, et de la Commission canadienne d'assurance emploi.

DRHC a comme mandat d'assurer un milieu de travail sécuritaire, sain et stable, de gérer les programmes de sécurité du revenu, et d'aider les Canadien(ne)s à se trouver un emploi et à le conserver. Cela signifie une clientèle et une charge de travail immenses, un budget gigantesque, et une quantité astronomique de renseignements personnels sur chaque habitant, ou presque. Mandat et responsabilités qui poussent DRHC à s'assurer à l'extrême que ses programmes sont bien gérés et que nul ne profite indûment du système.

Le ministère dépend énormément des technologies de l'information dans la prestation, le suivi et l'évaluation de ses programmes et services. Il serait impossible d'en faire autrement vu la charge de travail et les réductions d'effectifs. DRHC est également bien placé pour lancer de nouvelles applications de sa technologie. Il n'en reste pas moins que les gigantesques bases de données du ministère, ses puissants ordinateurs et les liens croissants qu'il tisse avec les provinces et le secteur privé dans la sous-

traitance de certains de ses services ont tout pour mériter les préoccupations du Commissariat à la protection de la vie privée.

Notre équipe de vérification a adopté une approche informelle mais systémique lui permettant d'avoir une vue d'ensemble du ministère. Nous avons identifié les renseignements personnels recueillis par le ministère, la raison de la collecte, les différents employés ayant accès à ces renseignements, les usages dérivés de ces derniers, les parties à qui ils sont communiqués, ainsi que le moment où ils sont détruits. Ensuite, nous nous sommes concentrés sur les activités du ministère posant le plus de risques pour la vie privée de ses clients : le projet de numéro unique d'identification des clients (voir plus haut), et le Fichier longitudinal sur la main-d'œuvre.

Le Fichier longitudinal sur la main-d'œuvre

Les uns après les autres, les commissaires fédéraux à la vie privée ont rassuré la population en lui disant que le gouvernement ne disposait d'aucun dossier unique sur eux. Nous avions tort… ou pas suffisamment raison, selon le cas.

Le fait de ne pas disposer de fichiers sur le client est une bonne chose : plus les bases de données sont distinctes, moins on risque de recueillir des renseignements sans discrimination, de les utiliser à des fins qui n'ont aucun rapport avec les fins initiales ou de les communiquer d'une façon non appropriée. Il est peut-être moins « efficient » d'organiser les informations en « silos » (bases de données distinctes), mais cela permet de davantage protéger la vie privée des gens, étant donné que le silo ne sert qu'à une fin bien précise. Statistique Canada est le seul organisme qui recueille plein de renseignements sur chacun de nous, mais ne le fait qu'à des fins statistiques, et non pour décider de notre sort. De plus, les données de Statistique Canada sont rigoureusement protégées. Les personnes qui en abusent sont passibles d'une amende et d'une peine d'emprisonnement.

La Direction générale des politiques stratégiques a élaboré le Fichier longitudinal sur la main-d'œuvre à des fins de recherche, d'évaluation, d'analyse de politiques et de programmes à l'appui des activités et services du Ministère.

Le Fichier longitudinal sur la main-d'œuvre est presque un fichier sur chaque citoyen. La base de données de recherche contient, pour près de 34 millions de personnes (aux dernières nouvelles), un dossier regroupant des données de fichiers gouvernementaux internes et externes très distincts et recueillis à différentes périodes. Les données ne sont jamais épurées, ce qui explique pourquoi il y a plus de dossiers que de Canadien(ne)s.

Le groupe de l'Exploitation des données et services techniques de la Direction générale des politiques stratégiques extrait des données recueillies auprès d'autres ministères fédéraux et d'autres ordres de gouvernement à l'aide de numéros d'identification uniques. Le groupe actualise fréquemment les bases de données pour que les renseignements en soient le plus à jour possible et reflètent les modifications apportées aux lois et aux procédures opérationnelles. Les données sont extraites de dossiers dans plusieurs programmes non reliés, notamment :

- les déclarations de revenus T1 et les formulaires connexes T4-S et T4-F ;
- la prestation fiscale pour enfants ;
- les dossiers sur les immigrants et les visiteurs (d'EIC, jusqu'en 1993) ;
- les dossiers provinciaux et municipaux du bien-être social ;
- le Programme national de formation ;
- la Planification de l'emploi ;
- le Service national de placement ;
- les dossiers administratifs de l'assurance emploi ;
- les relevés d'emploi ;
- le fichier maître de l'assurance sociale.

De plus, le ministère se propose d'élargir la base de données pour y intégrer des données provinciales et territoriales sur les prestataires d'aide sociale, ainsi que des données du Programme canadien de prêts aux étudiants, du Régime de pensions du Canada et de la Sécurité de la vieillesse.

Un dossier bel et bien unique

Une fois sa vérification terminée, le Commissaire à la protection de la vie privée a écrit à DRHC, expliquant ses grandes préoccupations face à ce qui n'est ni plus ni moins un dossier unique, complet, permanent et pratiquement invisible sur chaque habitant. Ont suivi nombre de lettres et d'appels téléphoniques de part et d'autre.

La collecte de données à des fins de recherche ne constitue pas obligatoirement une atteinte à la vie privée. Nombre de bases de données gouvernementales servent à des fins de recherche, et la *Loi sur la protection des renseignements personnels* traite spécifiquement de cette éventualité. Pourquoi alors se préoccuper du Fichier longitudinal sur la main-d'œuvre ?

Pour de nombreuses raisons. Commençons par son exhaustivité : il s'agit d'une base de données extraordinairement détaillée, qui pourrait contenir jusqu'à 2 000 éléments composites sur une personne, notamment la scolarité, l'état civil, la langue, la citoyenneté et le statut d'immigrant reçu, l'origine ethnique, la mobilité, les incapacités, le revenu, les antécédents professionnels, les activités sur le marché du travail, le recours à l'aide sociale et à l'assurance emploi. Le fait de centraliser et d'intégrer continuellement autant de données personnelles sur presque chaque habitant du Canada présente des risques importants pour la protection de notre vie privée.

Deuxièmement, la base de données est relativement invisible. Ce n'est pas que DRHC tente de cacher son existence. En fait, le ministère décrit la base de données dans le catalogue *InfoSource* et sur son site Web. Malheureusement, ni l'un ni l'autre ne sont facilement accessibles ni couramment consultés, et la description de la base de données contient peu de détails. Les Canadien(ne)s ne savent pas combien de renseignements sont recueillis ni à quel point ces renseignements sont intégrés et partagés. Combien de contribuables savent que leurs déclarations de revenus se retrouvent à DRHC ? Le ministère peut fournir les données sous contrat à des maisons de recherche privées à des fins de planification, de production de statistiques, de recherche et d'évaluation. Il peut communiquer les données à des organismes non gouvernementaux (comme des chercheurs et des universités) pour qu'ils mènent des études au nom de DRHC en vertu d'ententes officielles ou de contrats. De plus, certains organismes gouvernementaux (dont Statistique Canada ou les gouvernements provinciaux et territoriaux) peuvent utiliser certains renseignements pour mener des recherches sur la main-d'œuvre, le marché du travail et d'autres domaines connexes.

Troisièmement, la base de données est permanente. Elle n'est jamais épurée et contient des données allant de la naissance de quelqu'un à sa mort, sinon au-delà. Les bases de données de recherche devraient s'assortir de paramètres définis qui limitent la durée d'entreposage. Sans de telles limites, il est tentant de soumettre tout le monde à une surveillance continuelle. Cette base de données doit être circonscrite.

Quatrièmement, il n'existe pas de cadre législatif de protection. Statistique Canada, organisme gouvernemental prédominant en matière de statistiques, est tenu par des lois très strictes (qui prévoient des pénalités) de protéger les renseignements personnels qu'il recueille à des fins de recherche et de statistique. Il ne peut utiliser, partager ou vendre ces renseignements à des fins opérationnelles. Mais aucune mesure comparable ne protège les bases de données de recherche de DRHC.

La compilation de tels fichiers longitudinaux au moyen de couplage de dossiers menace notre vie privée car le gouvernement est tenté d'y recourir pour en analyser les données et les caractéristiques de certains individus. Une telle « base de données de recherche » peut rapidement se prêter à d'autres usages préoccupants, comme servir à prendre des décisions ou à faire des prédictions sur les gens ou à cibler défavorablement les gens d'une certaine ethnie ou souffrant de certains handicaps. Ces craintes sont fondées : rappelons-nous ce projet pilote que DRHC lançait voilà deux ans, servant à évaluer les conséquences des services du ministère, et qui se serait appuyé sur le Fichier longitudinal à des fins opérationnelles. Ce projet a été remis à plus tard face à la menace du changement de date du nouveau millénaire.

Nous avons fait part pour la première fois à DRHC de nos sérieuses préoccupations concernant le Fichier longitudinal sur la main-d'œuvre en septembre 1998, et nous continuons à le faire. Nous avons notamment recommandé au ministère :

- d'adopter une durée maximale de conservation des données du Fichier ;
- d'instaurer des sanctions contre tout usage abusif des données ;
- d'exclure les objectifs opérationnels des fins admissibles des données ;
- de strictement contrôler et protéger la collecte, l'usage et la conservation de toute donnée utilisée à des fins de recherche et d'évaluation ; et
- d'incorporer à sa loi habilitante un mandat de recherche spécifique et sans équivoque.

La réponse du ministère
Les responsables de DRHC se sont eux aussi penchés sur la taille du Fichier, les méthodes de collecte des données, la façon de prévenir la population des usages secondaires de ces données, et la permanence de ces dernières dans le Fichier. Le Commissariat a reçu une copie du rapport final de DRHC en septembre 1999.

La taille du Fichier : DRHC considère que tous les renseignements contenus dans le Fichier sont essentiels à l'élaboration des politiques du ministère, à la gestion de ses « interventions », à la conception de ses programmes et à la prestation de ses services. DRHC ne partage pas notre opinion de sa collecte comme étant spéculative mais nous fait remarquer qu'il serait illogique que le ministère recueille et conserve des renseignements qui lui sont inutiles ! Selon le ministère, les facteurs à prendre en ligne de compte dans une évaluation crédible des politiques sociales et de main-d'œuvre sont innombrables, et les données utilisées doivent identifier les personnes qu'elles

concernent afin que DRHC puisse cibler et évaluer des groupes ou des secteurs précis. Le ministère conclut en nous faisant remarquer que tous les renseignements du Fichier soit ont un lien avec ses activités soit peuvent lui être communiqués par d'autres organismes gouvernementaux en vertu de leurs lois, se conformant ainsi dans les deux cas à la *Loi sur la protection des renseignements personnels.*

Les méthodes de collecte : DRHC soutient que ses employés ne sont tenus de recueillir les renseignements de quelqu'un directement de cette personne que lorsque ces renseignements servent à des fins administratives, soit la prise de décisions affectant directement cette personne. Le Fichier ne servant pas à de telles fins, la collecte n'a donc pas besoin d'être directe. Le ministère poursuit en nous rappelant que la *Loi sur la protection des renseignements personnels* n'exige la collecte directe que si celle-ci est possible. Le Parlement aurait ainsi expressément autorisé des collectes indirectes telles celles nourrissant le Fichier, DRHC considérant l'alternative comme impossible. Le ministère conclut en nous rappelant que le paragraphe 8(2) de la Loi autorise un ministère à communiquer à des fins de recherche les renseignements personnels dont il a la charge.

L'avis donné à la population : Le ministère soutient qu'il n'est nullement obligé de prévenir la population de ses collectes indirectes puisque la *Loi sur la protection des renseignements personnels* n'exige un tel avis que dans le cas de collectes directes. Les renseignements recueillis provenant d'autres organismes fédéraux, et le Fichier ne servant pas à des fins administratives, DRHC maintient ne pas devoir prévenir la population. Le ministère s'est cependant engagé à réviser la description du contenu et de l'usage du Fichier qu'il publie dans le catalogue *InfoSource* et sur son site Web.

La durée de conservation des données : Le ministère a rejeté notre préoccupation à cet égard, prétextant un besoin d'analyser les données durant différents cycles du marché et d'évaluer l'impact de variables telles le libre-échange, l'évolution technologique et la globalisation des marchés. DRHC indique en conclusion que la *Loi sur la protection des renseignements personnels* ne fait nullement état de limites de conservation quant aux données de recherche.

La protection des données : Selon le ministère les lois et politiques internes actuelles suffisent à protéger les données du Fichier, dont les éléments permettant d'identifier les personnes sont cachés et d'accès limité. DRHC reconnaît cependant que les sanctions imposables aux contrevenants sont moindres que dans la *Loi sur la statistique* ou la *Loi sur l'impôt sur le revenu*, mais croit que le professionnalisme de son personnel et ses politiques internes

sont suffisantes.

DRHC conclut son rapport en alléguant qu'il respecte l'ensemble de la législation sur la vie privée et des lois et règlements connexes.

Depuis, cependant, le ministère a accepté de ne conserver les données du Fichier que 25 ans, de restreindre l'accès à ce dernier, et d'instaurer des mesures interdisant l'usage des données à des fins administratives. DRHC songe également à faire rajouter des pénalités et des sanctions à sa loi habilitante contre toute personne abusant des données.

Notre point de vue

Le Commissaire à la protection de la vie privée a félicité le ministère de ces derniers gestes, mais lui a fait remarquer que ces mesures protégeaient la sécurité des données, et non la vie privée des Canadien(ne)s. Le Commissaire trouve très difficile d'accepter, sur la base de l'examen de DRHC, que toutes les données du Fichier sont réellement pertinentes et nécessaires aux activités du ministère. Dans une autre lettre, le Commissaire a comparé le Fichier à un dossier unique sur chaque citoyen.

Le Commissaire n'a pas non plus accepté la remarque du ministère voulant que celui-ci se conforme à la *Loi sur la protection des renseignements personnels*. Qualifiant cette remarque d'une interprétation restreinte et littérale des droits fondamentaux stipulés dans la Loi, le Commissaire s'est dit insatisfait de l'attitude du plus gros ministère fédéral dont il croit que la création, l'entretien et l'alimentation de dossiers sur une majeure partie de la population constituent des activités ne pouvant pas simplement se suffire d'une conformité à un minimum d'exigences.

Si le ministère voulait vraiment se conformer à la Loi et se montrer honnête envers les citoyens, il devrait faire toute la lumière sur ses activités de recherche et son processus décisionnel. Les Canadien(ne)s devaient pouvoir savoir pourquoi leurs renseignements sont recueillis, à quoi ils serviront, combien de temps ils seront conservés et à qui ils seront communiqués. La réponse du ministère est donc inadéquate. DRHC a cependant offert de poursuivre le dialogue, et nous avons accepté. Le ministère passe de mauvais moments, et nous ne voulons pas rajouter à ses difficultés. Mais voilà plus de deux ans que nous avons lancé le débat, et il est grand temps d'y faire participer tous ces gens dont le ministère fouille les renseignements personnels à des fins de « développement de politiques sociales ».

Sur la colline

Afin de mieux protéger la vie privée de la population, le Commissariat fédéral à la protection de la vie privée suit de près les activités de la Chambre des communes et du Sénat, et tente d'étudier chacun des projets de loi débattus par ces deux chambres pour le cas où ces derniers auraient des incidences sur notre vie privée (ce qui n'est pas toujours facile à déterminer). Si ces incidences sont importantes, le Commissaire soumettra ses commentaires aux comités pertinents. Ce faisant, le Commissaire remplit son rôle de chien de garde parlementaire pour les questions de vie privée, contribuant aux connaissances de nos élus au besoin et leur recommandant la meilleure façon de minimiser ou d'éviter les incidences qu'il aura relevées.

Nouveaux projets de loi
Voici ceux des plus récents projets de loi déposés par le gouvernement qui ont des incidences sur la vie privée :

- La *Loi sur le recyclage des produits de la criminalité* (projet de loi C-22, anciennement C-81). Ce projet de loi vise l'instauration de mécanismes dissuasifs et répressifs reliés au blanchiment d'argent. Toute transaction suspecte devrait être rapportée, et un Centre d'analyse des opérations et déclarations financières du Canada verrait le jour qui filtrerait ces rapports et préviendrait le corps policier approprié ou l'Agence des douanes et du revenu du Canada de toute transaction justifiant enquête. Le Centre serait assujetti aux dispositions de la *Loi sur la protection des renseignements personnels*. Dans son dernier rapport annuel (aux pages 32 à 36), le Commissaire à la protection de la vie privée s'était penché sur l'ancienne version du projet (C-81) et croyait qu'il contreviendrait tant à la *Charte canadienne des droits et libertés* qu'à la *Loi sur la protection des renseignements personnels*. Le Commissaire se préoccupe également des critères qui rendraient une transaction « suspecte », ainsi que de la nature exacte du Centre. Ce projet de loi est étudié plus à fond ci-dessous.
- La *Loi sur le système de justice pénale pour les adolescents* (projet de loi C-3, anciennement C-68). Ce projet de loi remplacerait l'actuelle *Loi sur les jeunes contrevenants*, et comporte deux éléments qui préoccupent particulièrement le Commissariat à la protection de la vie privée : certaines communications de renseignements sur les contrevenants à leurs victimes ou au public, ainsi que l'analyse médico-légale d'échantillons génétiques de ces derniers. Ces deux nouveaux éléments pourraient réduire de façon appréciable le droit à la vie privée dont jouissent les jeunes contrevenants en vertu de la Loi actuelle.

- Le projet de loi S-10, modifiant la *Loi sur la défense nationale*, la *Loi sur l'identification par les empreintes génétiques* et le *Code criminel*. Ce projet de loi permettrait l'inclusion de renseignements sur les contrevenants militaires à la base de données génétiques nationale créée en 1998 en vertu de la *LIEG*, mais jusqu'ici réservée aux contrevenants civils. Le projet comporte deux éléments souhaitables, le premier limitant l'utilisation d'échantillons génétiques et de leur analyse aux fins d'application de la loi, le second obligeant le Commissaire de la Gendarmerie royale du Canada à soumettre au Solliciteur général un rapport annuel sur la gestion de la base de données génétiques nationale. Le Commissaire à la protection de la vie privée a cependant indiqué au Comité sénatorial permanent des affaires juridiques et constitutionnelles sa préoccupation à l'égard du nombre d'infractions permettant à un juge d'ordonner le prélèvement d'un échantillon génétique. Le Commissaire demeure en effet convaincu qu'un tel échantillon ne devrait être prélevé qu'une fois le contrevenant reconnu coupable d'une infraction accompagnée de violence, fortement présumé récidiviste, et susceptible ce faisant de laisser un échantillon génétique sur les lieux.

Certains autres projets de loi gouvernementaux ont également des incidences sur la vie privée :

- La *Loi électorale du Canada* (projet de loi C-2, anciennement C-83). Ce projet est une refonte de la loi actuelle et contient notamment des dispositions reliées au Registre national des électeurs. Les membres du Comité permanent de la Chambre des communes sur la Procédure et les Affaires de la Chambre ont approuvé une modification au projet qui permettrait la collecte du numéro de téléphone non-confidentiel de chaque électeur et sa transcription sur les listes électorales. Le Commissaire à la protection de la vie privée a demandé aux membres du comité de revenir sur leur décision, et leur a recommandé d'obliger le Directeur général des élections à prévenir chaque électeur du fait que ses renseignements personnels pourraient être utilisés par les partis politiques qui souhaiteraient recruter de nouveaux membres ou obtenir des contributions à leur caisse.
- La *Loi sur l'Accord définitif Nisga'a* (projet de loi C-9). Ce projet de loi officialisera l'accord d'autonomie gouvernementale survenu récemment entre le gouvernement fédéral et le peuple Nisga'a. La *Loi sur la protection des renseignements personnels* sera également modifiée pour rajouter les gouvernements autochtones à la liste des organismes auxquels une institution fédérale peut communiquer nos renseignements personnels sans notre consentement.

- La *Loi sur la citoyenneté du Canada* (projet de loi C-16). Ce projet remplacerait l'actuelle *Loi sur la citoyenneté* et codifierait notamment la pratique courante voulant que le Ministre de la citoyenneté et de l'immigration communique les noms de nouveaux citoyens canadiens aux Sénateurs et aux députés fédéraux afin que ceux-ci félicitent ces derniers. À l'heure actuelle, le Ministre doit obtenir l'approbation préalable du nouveau citoyen avant de communiquer son nom. Mais le projet de loi permettrait une telle communication de façon courante, à moins que le nouveau citoyen ne s'y objecte. Un tel renversement d'optique va à l'encontre des règles de protection de la vie privée et n'est pas sans rappeler les stratégies tant décriées de ces câblodistributeurs qui facturent leurs clients pour de nouveaux postes que ces derniers n'ont pas expressément demandés. Le Commissaire à la protection de la vie privée a écrit au Ministre pour lui faire part de son point de vue à cet égard.
- La *Loi sur les instituts de recherche en santé du Canada* (projet de loi C-13). Ce projet permettrait la création d'instituts de recherche virtuels (soit de simples regroupements de chercheurs sans lieu de travail commun) qui fourniraient de nouvelles connaissances en santé et convertiraient ce savoir en un système national amélioré de prestation de meilleurs soins de santé. Le Commissariat s'inquiète particulièrement du risque très réel que les chercheurs de ces instituts obtiennent accès à quantité de renseignements personnels sur chacun de nous sans que nous le sachions et sans notre consentement.

Projets de loi un peu moins récents

Les projets de loi suivants ont été entérinés lors de la dernière année :

- La *Loi de mise en œuvre de l'Accord sur la Station spatiale internationale civile* (projet de loi C-4, anciennement C-85). Ce projet de loi donne vie à l'accord international récemment survenu sur la construction et les activités de la future station spatiale civile. Ce projet, qui a reçu la sanction royale en décembre 1999, contient des dispositions permettant le partage international de renseignements personnels à des fins d'application de la loi.
- Le projet de loi C-7 (anciennement C-69), modifiant les dispositions du *Code criminel* ayant trait aux réhabilitations. Entre autres, le projet de loi C-7 permettra qu'apparaisse aux dossiers du Centre canadien d'information de la police une mention de toute réhabilitation accordée à un ancien délinquant sexuel (le CCIP, géré par la GRC, est accessible à tous les corps policiers du pays). Cette réhabilitation, jusqu'ici secret inaccessible, pourra alors être divulguée dans le cadre d'une vérification de la fiabilité de l'ancien délinquant si celui-ci postule un emploi le mettant en contact

avec des enfants ou d'autres personnes à risque. Ce projet a été adopté par le Sénat en décembre 1999.

- Le projet de loi C-43, remplaçant l'ancien ministère du Revenu par une nouvelle Agence des douanes et du revenu du Canada. Les préoccupations du Commissariat à la protection de la vie privée découlaient de l'immense quantité de renseignements très personnels sur chaque contribuable dont l'Agence a hérité. Cette dernière est assujettie aux dispositions de la *Loi sur la protection des renseignements personnels*. Ce projet a reçu la sanction royale en avril 1999, et est entré en vigueur en novembre de la même année.

- Le projet de loi C-67, portant sur les institutions financières étrangères ayant des succursales au Canada. Ce projet de loi traitait notamment de l'utilisation et de la communication de renseignements personnels des clients de ces institutions, ainsi que des pratiques de vente liée. Ce projet a reçu la sanction royale en juin 1999.

- Le projet de loi C-71, mettant en œuvre le budget fédéral de 1999. L'unique incidence de ce projet de loi sur la vie privée visait le partage de renseignements fiscaux aux fins de prestations suite à un accident de travail. Ce projet a reçu la sanction royale en juin 1999.

- Le projet de loi S-22, permettant aux responsables américains de pré-contrôler les voyageurs à destination de notre voisin du sud par le biais ou en provenance du Canada. Les deux principales incidences de ce projet avaient trait à la protection disponible en sol canadien du fait de lois canadiennes telles la *Loi sur la protection des renseignements personnels*, ainsi que le recours à des fiches détaillées sur les préférences et les agissements de chaque voyageur. Ces préoccupations ont été soulevées dans le dernier rapport annuel du Commissaire à la protection de la vie privée, aux pages 38 à 40. Ce projet a reçu la sanction royale en juin 1999.

Motions et projets de loi d'intérêt privé

Les lois canadiennes ne tirent pas toujours leur source du gouvernement fédéral et de ses ministères, cependant. En effet, le système parlementaire canadien permet à tout député ou sénateur ne faisant pas partie du Cabinet de déposer son propre projet de loi. Et la dernière année a été particulièrement riche en projets de loi et en motions ayant des incidences sur notre vie privée. À preuve :

- Le projet de loi C-270 (du député Jim Pankiw) interdirait la publication du nom d'un accusé avant que celui-ci ne soit reconnu coupable ou innocenté.

- Le projet de loi C-393 (du député Mac Harb) obligerait les institutions

financières de compétence fédérale, les sociétés incorporées sous régime fédéral et les bureaux de crédit à prévenir tout consommateur dont ils s'apprêtent à communiquer l'historique financier à un fournisseur ou un bureau de crédit. Le projet permettrait également aux consommateurs de se plaindre auprès du Surintendant des institutions financières.

- Le projet de loi C-395 (du même député) limiterait l'usage de notre numéro d'assurance sociale aux organismes en ayant reçu l'autorisation juridique expresse.
- Le projet de loi C-417 (du député Greg Thompson) donnerait notamment aux patients le droit d'accéder à leur dossier médical, de le corriger au besoin et d'en contrôler la communication.
- Le projet de loi C-419 (du député Bill Gilmour) permettrait à quiconque refuse de recevoir des appels ou des télécopies de télémarketing d'inscrire son numéro de téléphone à une liste que gèrerait le Conseil de la radiodiffusion et des télécommunications canadiennes. Les vendeurs ne tenant pas compte de cette liste commettraient une infraction et se verraient imposer une amende.

N'oublions pas non plus la Motion M-19 (du député Mike Scott), qui faisait écho à nos instances en vue de la refonte tant espérée de la *Loi sur la protection des renseignements personnels* (traitée dans une autre section de ce rapport annuel). Cette motion aurait permis à un comité de la Chambre des communes de déposer un projet de loi étoffant les pénalités retenues par la *LPRP*. Ces dernières auraient notamment compris l'octroi de dommages-intérêts à toute personne lésée par la communication abusive de ses renseignements personnels, ainsi que l'imposition de sanctions aux contrevenants. Cette motion est malheureusement morte au feuilleton après un bref débat.

Tous les projets de loi d'intérêt privé ne font pas autant avancer notre cause, cependant, tels ceux visant l'application de la loi. Les députés Myron Thompson et Chuck Strahl ont tous deux déposé des projets permettant à un policier d'exiger, respectivement, un échantillon d'urine de tout conducteur simplement *soupçonné* de conduite dangereuse (projet C-234) ou un échantillon de sang de toute personne *soupçonnée* être porteuse d'un virus (projet C-244). Les projets de loi C-262 du député Peter MacKay et C-264 du député Keith Martin sont pratiquement identiques.

Deux autres projets de loi déposés cette année et ayant des incidences négatives sur notre vie privée traitent d'un sujet soulevé ailleurs dans ce rapport ainsi que dans le dernier rapport annuel du Commissaire à la

protection de la vie privée (aux pages 27 à 29) : l'accès aux données du recensement. Le Commissaire s'est toujours opposé à la divulgation publique de tout renseignement permettant d'identifier la personne qu'il concerne et obtenu lors de recensements en vertu des dispositions expresses de confidentialité de la *Loi sur la statistique*. Mais tant la sénatrice Lorna Milne que le député Mac Harb ont déposé des projets de loi (respectivement numérotés S-15 et C-312) qui obligeraient Statistiques Canada à transférer aux Archives nationales du Canada toutes les données des recensements de 1906 et des années suivantes. Les Archives mettraient ensuite ces données à la disposition du public 92 ans après leur collecte initiale. Le député Jason Kenney a quant à lui déposé sa Motion M-160, demandant la divulgation publique des données du recensement de 1911 dès leur transfert aux Archives nationales en 2003.

Faisons en terminant une brève mention du projet de loi C-264 du député John Bryden. Ce projet modifierait la *Loi sur l'accès à l'information* et obligerait une institution fédérale à communiquer à un requérant tout renseignement vieux de plus de 30 ans (y compris un renseignement personnel d'un tiers) ou tout renseignement pouvant légalement être communiqué, et ce même si l'institution est d'avis que le renseignement devrait rester confidentiel. La divulgation automatique de tout renseignement personnel vieux de plus de 30 ans court-circuiterait complètement la *Loi sur la protection des renseignements personnels*, laquelle exige le consentement préalable d'une personne à la communication de ses données, à moins de dispositions contraires dans une autre loi ou si la personne est décédée depuis plus de 20 ans. La divulgation automatique de tout renseignement pouvant être légalement communiqué éliminerait cette faculté essentielle qu'ont à l'heure actuelle les institutions fédérales et qui leur permet de s'opposer à la communication de tels renseignements si elles en jugent ainsi. Dans les deux cas, ce projet risque donc de nuire à notre vie privée. Le Commissaire à la protection de la vie privée appuie certes l'objectif visé par M. Bryden, soit celui d'un gouvernement fédéral plus redevable et moins secret. Le Commissaire, cependant, croit que ce projet devrait être modifié de sorte à ne pas s'appliquer à nos renseignements personnels.

Comment dépister les incidences d'un projet de loi sur la vie privée ?
Voici certaines des questions que se pose le personnel du Commissariat à la protection de la vie privée lors de son étude de chaque projet de loi. Ce dernier :

- fait-il spécifiquement référence à la *Loi sur la protection des renseignements personnels* ou à la Loi C-6 ?
- crée-t-il ou abolit-il une institution assujettie à la *Loi sur la protection des*

renseignements personnels ?

- crée-t-il, change-t-il ou abolit-il une collecte de nos renseignements personnels (tel le Registre des armes à feu) ?
- fait-il état de pouvoirs de perquisition ou de saisie (tel le prélèvement d'échantillons génétiques) ?
- permet-il, directement ou non, le suivi ou la surveillance d'individus ?
- crée-t-il, modifie-t-il ou abolit-il un partage ou un couplage de nos renseignements personnels ?
- propose-t-il une nouvelle utilisation de renseignements personnels déjà recueillis ?
- accorde-t-il à une institution le droit d'accéder à nos renseignements personnels ?
- élargit-il, restreint-il ou interdit-il la communication de nos renseignements personnels ?
- exige-t-il la publication ou la disponibilité publique de nos renseignements personnels ?
- impose-t-il des frais ou d'autres obstacles à notre accès à nos propres renseignements personnels ?
- exige-t-il la conservation de nos renseignements personnels pendant un certain temps ?
- requiert-il la destruction de nos renseignements personnels ?
- considère-t-il comme une infraction la collecte, l'utilisation ou la communication abusive de nos renseignements personnels ?
- propose-t-il une nouvelle technologie susceptible de porter atteinte à notre vie privée ?

Le point sur la *Loi sur le recyclage des produits de la criminalité*

Dans le rapport annuel de l'an dernier, nous avons rapporté l'intention du gouvernement de renforcer et de moderniser la législation actuelle sur la détection, la poursuite et la dissuasion des activités illicites de blanchiment d'argent. Cette intention s'est concrétisée dans le projet de loi C-22, la *Loi sur le recyclage des produits de la criminalité*, présentement à l'étude devant la Chambre des communes. Nous avions plusieurs préoccupations face aux incertitudes entourant des éléments clés de la Loi. Certaines de ces incertitudes devraient

être précisées dans le cadre d'un règlement, mais d'autres ne seront pas dissipées.

L'une de ces préoccupations est que nul ne sait encore si les personnes ou les entités assujetties à la Loi (telles les banques et les maisons de courtage) seront tenues d'informer un client et d'obtenir son consentement pour recueillir ceux de ses renseignements exigés par la Loi, ou pour les communiquer au Centre d'analyse des opérations et déclarations financières du Canada (le « Centre »). Se pourrait-il aussi que ces personnes ou entités s'abstiennent régulièrement d'aviser leurs clients pour la simple raison que cela pourrait nuire à l'usage des renseignements à des fins d'enquête, qu'une enquête policière officielle ait été engagée ou non ? Le fait d'informer au préalable un client des fins pour lesquelles on recueille des renseignements à son sujet constitue un principe clé de la protection des données, qui pourrait ne pas être adéquatement respecté dans le projet de loi C-22.

Alors que l'exigence de recueillir certains renseignements comme le montant d'argent et les coupures en jeu devrait aller de soi pour les parties qui prennent part à la transaction, la nécessité de recueillir d'autres renseignements pour évaluer de façon appropriée si la transaction est louche ne saute pas immédiatement aux yeux. En effet, le gouvernement n'a pas encore précisé les renseignements qui pourraient servir à éclairer les circonstances d'une transaction ou permettre à la personne recevant l'argent de confirmer la véracité des dires de la personne lui remettant cet argent. Le gouvernement a l'intention de fournir ces précisions sous forme de lignes directrices qui seront développées au besoin par le Centre et les entreprises privées assujetties aux nouvelles exigences.

"CE FORMULAIRE NOUS ENGAGE À NE JAMAIS DIVULGUER VOS RENSEIGNEMENTS PERSONNELS À MOINS D'AVOIR UN SOLIDE INCITATIF FINANCIER POUR LE FAIRE!"

Notre dernier rapport annuel mettait le lecteur en garde contre la possibilité que le personnel de ces entreprises soit appelé à prendre des décisions hautement subjectives à l'endroit de certains clients et des circonstances entourant leurs transactions. Nous craignions aussi que ce personnel ne se

voie chargé de confirmer une première impression en fouillant plus avant dans la vie ou la transaction d'un client, devenant par le fait même des enquêteurs au service de l'État. Nous favorisons donc une approche reposant sur des critères simples et objectifs reliés à la transaction, et qui seraient inclus dans un règlement, et non de simples lignes directrices.

Il nous manque plusieurs réponses, à commencer par les éléments de données qui entraîneraient l'obligation de déclarer au Centre une transaction donnée. Un simple seuil monétaire ne provoquerait pas obligatoirement de déclaration, et pourrait même ne pas du tout s'appliquer dans certaines transactions. Par exemple, dans un cas où un client a payé plus que le taux de change affiché ou plus que les frais de transaction pour faciliter une transaction par mandat, cela suffirait-il en soi pour déclencher une déclaration, quels que soient les montants d'argent en jeu ?

Les règlements préliminaires ont établi deux critères repères à ce sujet : au moins deux transactions menées la même journée totalisant une rentrée de fonds de 10 000 $ comptant ou plus, ainsi que toute transaction mettant en jeu cinq billets de 1 000 $ ou plus. Ce dernier critère représente une réduction importante du seuil monétaire où l'on doit déclarer une transaction. Même s'il permettait de détecter de petits criminels, ce seuil monétaire moins élevé déclenchera aussi la déclaration de nombreuses transactions innocentes. (Indépendamment de cette Loi, le gouvernement a déjà pris des mesures pour contrer le blanchiment d'argent en annonçant que la Banque du Canada n'émettra plus de billets de 1 000 $.)

Bien sûr, le simple fait de déclarer au Centre une transaction jugée louche ne donne pas nécessairement lieu à une enquête officielle. Pour évaluer s'il y a des motifs raisonnables de croire que l'argent découle d'activités criminelles, le Centre doit analyser ces renseignements relativement aux informations glanées d'autres sources, notamment les renseignements fournis au Centre concernant le suspect et les renseignements obtenus auprès des forces de l'ordre ou d'autres organismes gouvernementaux et pertinents au blanchiment d'argent.

Si la notion de « renseignement pertinent au blanchiment d'argent » peut englober tout renseignement permettant de conclure ou non aux activités criminelles ou illicites d'un suspect, il n'y aura véritablement pas de limites aux renseignements que recevra le Centre. De plus, ce dernier pourrait compléter le dossier criminel d'un suspect par des renseignements sur les antécédents professionnels, financiers et de voyage de ce suspect, sans oublier ses revenus, ses affiliations ou relations professionnelles, et même ses relations personnelles.

Le Commissariat croit que ces catégories de renseignements et leurs sources devraient être clairement spécifiées dans la Loi ou son règlement. Ceci limiterait ainsi les renseignements recueillis par le Centre à ceux directement reliés et reconnus nécessaires à l'exercice de son mandat.

Une fois que le Centre a confirmé la nature criminelle d'une transaction, son personnel est autorisé à communiquer certains « renseignements désignés » à des organismes spécifiés, notamment la police ou la Gendarmerie royale du Canada, l'Agence des douanes et du revenu du Canada, le Service canadien du renseignement de sécurité et le ministère de la Citoyenneté et de l'Immigration. L'on entend actuellement par « renseignements désignés » des renseignements clés qui permettent d'identifier un suspect, comme son nom, la date et l'endroit où la transaction a eu lieu, le numéro de compte et la valeur de la transaction.

Le danger existe que l'on élargisse l'éventail de ces éléments de données pour inclure d'autres renseignements concernant la transaction. Le Commissariat à la protection de la vie privée maintient qu'on ne doit recueillir qu'un strict minimum de « renseignements désignés ». Autrement, le Centre pourrait ne devenir qu'un simple pipeline acheminant des preuves judiciaires aux forces de l'ordre, contournant ainsi les normes et les procédures rigoureuses qui s'appliquent actuellement à la collecte d'éléments de preuve dans le cadre d'enquêtes criminelles.

Même si le Centre est explicitement assujetti à la *Loi sur la protection des renseignements personnels* fédérale, une grande question reste sans réponse : quels droits une personne peut-elle exercer quant aux renseignements personnels détenus par le Centre ? Par exemple, la nouvelle *Loi sur le recyclage des produits de la criminalité* tiendra-t-elle compte des droits actuels que la *Loi sur la protection des renseignements personnels* accorde à chacun de consulter et de corriger ses renseignements personnels détenus par une institution fédérale ? Ou ces droits seront-ils refusés régulièrement parce que les renseignements ont été obtenus au cours d'une enquête judiciaire ? Nous ne pouvons qu'espérer que la *Loi sur la protection des renseignements personnels* aura préséance.

Dédouanement et vie privée des passagers

Dans le rapport annuel de l'an dernier, la section traitant de la *Loi sur le pré-contrôle* relatait la possibilité qu'ont les douaniers américains d'obtenir de transporteurs aériens des renseignements sur les voyageurs qui traversent le Canada pour se rendre aux États-Unis d'Amérique. Les douaniers américains en poste dans les principaux aéroports canadiens peuvent ainsi apprendre où

un passager a effectué sa réservation, comment il a réglé le coût de son billet, les repas spéciaux qu'il a demandés et le siège qu'il a réservé, tout cela pour aider les douaniers à décider s'ils doivent lui interdire d'entrer dans leur pays. Bien que les douaniers canadiens ne soient pas autorisés à se servir de tels renseignements à ces mêmes fins, la *Loi sur le pré-contrôle* permettaient à leurs homologues américains d'en faire ainsi en sol canadien. Nous nous préoccupions alors du précédent que les douanes canadiennes voudraient peut-être imiter.

Et nous avions bien raison. Nous avons appris depuis que Citoyenneté et Immigration Canada (CIC) et l'Agence des douanes et du revenu du Canada (ADRC) cherchaient à établir un système similaire d'établissement de profils de passagers dans le but d'accélérer le processus de dédouanement.

Dans le cadre du plan proposé, les renseignements personnels et les renseignements sur les déplacements de chaque passager seraient recueillis par les transporteurs aériens commerciaux qui les feraient parvenir aux fonctionnaires canadiens des douanes et de l'immigration à l'aéroport de destination avant l'arrivée des passagers. L'information servirait à créer un profil identifiant les voyageurs présentant un « risque élevé », lesquels seraient alors soumis à une interrogation « primaire » ou « secondaire ». La proposition originale reconnaissait que des modifications devraient être apportées tant à la *Loi sur les douanes qu'*à la *Loi sur l'immigration* avant la mise en œuvre du projet.

Notre personnel s'est penché sur la proposition et a découvert qu'un grand nombre de données — 32 au total — semblait nécessaire pour permettre aux fonctionnaires des douanes et de l'immigration d'identifier de façon efficace les « voyageurs suspects ». L'information demandée incluait non seulement le nom, la citoyenneté, le numéro du passeport, la date de l'achat du billet, l'historique du voyage et le pays de départ, mais aussi des renseignements portant sur le style de vie des passagers : quantité de bagages enregistrés, préférences alimentaires, et même si les repas avaient été consommés ou non. Nous nous sommes alors interrogés sur la pertinence de certains renseignements pour évaluer adéquatement le droit d'une personne à entrer au

Vivre en fonction du pire scénario, c'est comme accorder la victoire aux terroristes sans qu'un seul coup de feu n'ait été tiré. Il est aussi alarmant de penser que les vraies batailles du nouveau siècle pourraient se livrer en secret, entre des adversaires qui ne rendent de comptes à presque personne, les uns se targuant d'agir en notre nom, les autres espérant nous soumettre par la terreur.

— Salman Rushdie, 2000

Canada, ainsi que sur la capacité d'un transporteur aérien à fournir toute l'information demandée.

Nos longues consultations avec les fonctionnaires de CIC et de l'ADRC ont permis d'éliminer bon nombre d'éléments de données non appropriés et portant atteinte à la vie privée, le nombre total d'éléments passant de 32 à 15. Nous avons également demandé à CIC de nous expliquer la notion d' « historique de voyage », que nous voudrions voir limitée aux annulations et aux départs ratés.

Les renseignements personnels visés étant nombreux, et la création de profils présentant certains dangers, nous avons recommandé aux deux institutions de faire inscrire les éléments de données dans une loi et non dans des règlements. Nous leur avons également conseillé de modifier la *Loi sur l'immigration* et à la *Loi sur les douanes* pour clairement y interdire l'usage des données précédentes à des fins secondaires ou non pertinentes. Finalement, puisque ce programme est censé faciliter les déplacements des passagers, nous avons proposé que ces derniers restent libres d'y adhérer ou non. S'ils refusent, ils continueront le processus actuel de dédouanement et d'immigration, parfois plus lent. La proposition actuelle donne cependant au transporteur aérien le droit de décider à la place des passagers.

Renseignements sur les contribuables, ou statistiques ?

En mai 1999, le ministère des Finances et du Revenu du Canada (maintenant l'Agence des douanes et du revenu du Canada) a informé le Commissaire à la protection de la vie privée des modifications proposées à la *Loi de l'impôt sur le revenu* et la *Loi sur la taxe d'accise*, qui permettraient de communiquer des renseignements sur les contribuables aux organismes provinciaux responsables des statistiques.

Au début, le gouvernement a proposé de faire un ajout au paragraphe 241(4) de la *Loi de l'impôt sur le revenu* (et au paragraphe 295(5) de la *Loi sur la taxe d'accise*), lequel se lirait comme suit :

> « Un employé peut fournir des renseignements sur un contribuable à un autre employé uniquement aux fins de permettre à un organisme provincial responsable des statistiques d'obtenir des données statistiques pour la recherche et l'analyse et, nonobstant l'alinéa 17(2)a) de la *Loi sur la statistique*, dans le cas des renseignements sur un contribuable fournis par le Statisticien en chef, sans égard au moment où les renseignements ont été recueillis. »

Nous étions préoccupés par les répercussions que pourrait avoir cette modification sur la communication de renseignements personnels au sujet des contribuables. Un examen plus poussé a révélé les faits suivants :

- La modification vise à permettre à Statistique Canada de fournir aux organismes provinciaux responsables des statistiques de l'information financière sur les entreprises constituées en société et celles qui ne le sont pas, renseignements qu'il obtient de l'Agence des douanes et du revenu du Canada.
- Pour les organismes provinciaux responsables de statistiques, Statistique Canada a toujours représenté une source clé de données sur les entreprises canadiennes. Statistique Canada s'appuie sur des ententes de partage pour fournir aux provinces les renseignements dont elles ont besoin pour examiner et analyser les activités sociales et économiques.
- Les provinces ont de plus en plus besoin de renseignements financiers détaillés sur les petites et moyennes entreprises pour améliorer leurs statistiques économiques. Statistique Canada utilise davantage les dossiers de l'impôt sur le revenu plutôt que d'interroger directement les entreprises, ce qui réduit le fardeau de la réponse.
- Statistique Canada partagerait ses données avec les organismes provinciaux régis par des lois provinciales sur la statistique et qui sont donc assujettis à des modalités sévères de l'usage des données.
- Le gouvernement n'a pas du tout l'intention de partager des renseignements fiscaux sur des particuliers, à moins que ceux-ci n'aient fourni de l'information sur l'exploitation d'une entreprise dans leur déclaration de revenu.
- Les provinces accéderaient aux données sur l'impôt des sociétés grâce aux dispositions d'une ordonnance de communication discrétionnaire signée par le Statisticien en chef en vertu du paragraphe 17(2)*a*) de la *Loi sur la statistique*. La politique de Statistique Canada sur de telles ordonnances exige que la partie qui obtient des données s'engage à en préserver la confidentialité et à n'utiliser les renseignements qu'à des fins statistiques et de recherche. L'engagement empêcherait toute autre communication de données sans l'autorisation expresse du Statisticien en chef, et toute communication subséquente serait également contrainte par les dispositions de la *Loi de l'impôt sur le revenu*.

Le Commissaire à la protection de la vie privée a formulé quatre recommandations au ministère des Finances, à Statistique Canada et à l'Agence des douanes et du revenu du Canada :

- contrairement au libellé proposé, la modification devrait préciser le fait que l'information devant être communiquée concerne des entreprises ou des particuliers qui ont fourni dans leur déclaration de revenu des renseignements sur l'exploitation d'une entreprise;
- idéalement, Statistique Canada devrait ne fournir que les renseignements ultérieurs à l'entrée en vigueur de la modification — il ne devrait y avoir aucun effet rétroactif, ou, à la limite, la modification devrait préciser une année;
- des dépliants devraient indiquer aux contribuables, surtout les petites et moyennes entreprises, qui a accès à leurs renseignements fiscaux, et à quelles fins;
- les ententes conclues entre Statistique Canada et ses homologues provinciaux devraient clairement stipuler que les renseignements statistiques doivent être utilisés uniquement à des fins de recherche et d'analyse, et ce que la loi provinciale permette ou non d'autres usages administratifs.

Après force débats, toutes les parties ont accepté les recommandations. Les représentants de Statistique Canada et de l'Agence des douanes et du revenu du Canada élaborent actuellement les meilleurs mécanismes rentables permettant d'informer les Canadien(ne)s de l'usage prévu pour les données fiscales des entreprises. On les avisera une fois que la modification législative aura reçu la sanction royale. Même si le gouvernement a récemment décidé de ne pas modifier la *Loi sur la taxe d'accise*, il a changé le libellé de la modification du paragraphe 241(4) de la *Loi de l'impôt sur le revenu*. Ce dernier ressemblera sensiblement à ce qui suit :

> « Un employé peut fournir à un autre employé des renseignements sur le contribuable relativement à l'exercice 1997 ou à des exercices ultérieurs uniquement aux fins de permettre au Statisticien en chef de fournir à un organisme provincial responsable des statistiques des données statistiques qui seront utilisées pour la recherche et l'analyse, si l'information a trait :
>
> - à une société, ou
> - au calcul des revenus d'entreprise d'un particulier qui, selon une déclaration de revenu produite par celui-ci ou un avis de cotisation ou de nouvelle cotisation qui le concerne, a exploité une entreprise à n'importe quel moment au cours de l'exercice 1997 ou des exercices suivants, et, nonobstant l'alinéa 17(2)a) de la *Loi sur la statistique*, sans égard au moment où les renseignements ont été recueillis. »

Ces modifications constituent un excellent exemple de la façon dont le gouvernement peut améliorer notre vie privée et son administration en consultant le Commissariat à la protection de la vie privée lorsqu'il envisage de conclure de nouvelles ententes de partage de données touchant la population. La modification que l'on propose d'apporter à la *Loi de l'impôt sur le revenu* est désormais beaucoup plus précise et empêche toute mauvaise interprétation de sa portée et de son objectif prévus.

La modification proposée sera incluse dans le projet de loi du budget de cet automne.

Combler les lacunes : Une charte des droits relatifs à la vie privée

L'un des objectifs du Commissaire à la protection de la vie privée pendant la dernière décennie a été de combler certaines des lacunes en termes de protection de la vie privée au Canada.. L'adoption de la Loi C-6 a répondu à un manque d'importance : la *Loi sur la protection des renseignements personnels et les documents électroniques* confèrera aux Canadien(ne)s de nouveaux droits d'une grande portée en ce qui concerne la collecte, l'utilisation et la communication de renseignements personnels par le secteur privé.

Si l'adoption de la Loi C-6 représente un jalon de taille dans l'évolution de la protection de la vie privée au Canada, la victoire n'est pas encore acquise : le droit de la population à la vie privée n'est toujours pas garanti par la Constitution. Mais cela pourrait changer avec la charte des droits relatifs à la vie privée que propose la sénatrice Sheila Finestone.

Le projet de charte de la sénatrice Finestone donnerait à chacun le droit à sa vie privée. Toute intrusion dans la vie privée de quelqu'un serait considérée comme une violation de ce droit, à moins que l'intrusion ne soit raisonnablement justifiée et que le consentement de l'intéressé(e) n'ait été obtenu (sauf s'il est impossible ou inopportun d'obtenir celui-ci). Il incomberait alors à l'organisation ou la personne proposant l'intrusion de prouver que celle-ci est justifiée. La charte prévoirait des critères de raison applicables à la justification et elle obligerait le ministre de la Justice à examiner tous les projets de loi et de règlements déposés par le gouvernement pour s'assurer qu'ils respectent la charte. Toute anomalie à cet égard devrait être signalée au Parlement et au Commissaire à la protection de la vie privée, une mesure réclamée depuis longtemps par ce dernier.

Selon la sénatrice Finestone, la charte représenterait un vaste cadre relatif aux

droits en matière de vie privée pour le Canada. D'après nous, ceci revient à dire que la charte serait un ensemble de principes fondamentaux qui sous-tendrait tant la *Loi sur la protection des renseignements personnels* fédérale que la nouvelle loi visant le secteur privé. En effet, une institution gouvernementale peut à l'heure actuelle contourner la protection de la vie privée offerte par la *Loi sur la protection des renseignements personnels* si une autre loi l'y autorise expressément (alinéa 8(2)*b*) de la Loi). La charte obligerait l'institution à justifier la nécessité de l'atteinte à la vie privée que provoquerait l'adoption de l'autre loi. De plus, la charte offrirait des recours pour les personnes dont la vie privée est menacée par cette autre loi, telle la possibilité de contester la loi : un pas de plus vers notre objectif d'asseoir la primauté de la *Loi sur la protection des renseignements personnels* par rapport à toutes les autres lois fédérales visant la collecte, l'utilisation et la communication de renseignements personnels.

> *Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique.*
>
> — Gérard La Forest, 1988
> (R. c. Dyment)

La charte proposée contribuerait grandement à l'atteinte d'un autre de nos buts, soit l'inclusion dans la Constitution d'un droit à la vie privée. En 1991, le Commissaire à la protection de la vie privée a comparu devant le Comité mixte spécial sur le renouvellement du Canada pour réclamer l'ajout à la *Charte canadienne des droits et libertés* d'un tel droit. Vu la réticence probable de tout gouvernement à modifier la Charte dans un proche avenir, le document de la sénatrice Finestone constitue une solution de rechange que nous appuyons avec enthousiasme.

Madame Finestone est l'une des plus grandes alliées de la vie privée qui se trouvent dans la capitale. Parmi ses nombreuses réalisations, soulignons sa présidence du Comité permanent de la Chambre des communes sur les droits de la personne et la condition des personnes handicapées. En 1997, le rapport du Comité intitulé *La vie privée : où se situe la frontière ?* apportait des arguments judicieux et convaincants pour la reconnaissance de l'importance fondamentale de la vie privée dans la société canadienne grâce, entre autres, à l'adoption d'une charte canadienne des droits relatifs à la vie privée. Nous nous réjouissons de voir que l'arrivée au Sénat de Madame Finestone n'a en rien diminué son ardeur à défendre notre cause.

Direction de l'Analyse et de la gestion des enjeux

La direction de l'Analyse et de la gestion des enjeux étudie les programmes et les lois du gouvernement, effectue de la recherche sur les questions de l'heure, conseille le Commissaire en matière de politiques et l'appuie dans le domaine des communications.

Un petit groupe de chefs de portefeuille sert de point de référence aux agences fédérales afin de résoudre toute question avant qu'elle ne mène à une plainte. En outre, les chefs de portefeuille effectuent des vérifications officielles et des suivis.

Une poignée d'analystes a la responsabilité de garder le Commissariat au courant de tout événement affectant la vie privée. Cela comprend l'examen de projets de loi et de programmes gouvernementaux, la recherche de tendances canadiennes et étrangères, l'étude — à la demande d'autres organismes — de propositions affectant la vie privée, ainsi que la préparation de renseignements de fonds pour les communications publiques qu'effectue le Commissaire.

Les activités de communications et de suivi parlementaire de la Direction font mieux connaître le Commissaire. Préparer celui-ci pour des comparutions devant les comités parlementaires, rédiger des discours et la majeure partie du rapport annuel, et préparer les documents affichés sur le site Web du Commissariat comptent parmi les principales fonctions de la Direction.

Enfin, le personnel de la Direction étudie certaines questions plus complexes ne relevant pas directement du mandat du Commissaire. Il agit aussi comme point de contact pour les responsables étrangers de la protection des renseignements personnels s'intéressant à la situation canadienne en matière de protection de la vie privée, et appuie la direction des Enquêtes en lui fournissant les renseignements de fonds et en obtenant les avis juridiques qui s'avèrent nécessaires.

Les études d'impact sur la vie privée

Au cours des dernières années, la société canadienne a subi de nombreux changements : croissance démographique rapide, exigences accrues imposées aux ressources de l'État, privatisation des activités gouvernementales et

développement et disponibilité exponentiels des technologies de l'information et de communication.

De nouveaux programmes, produits, services et technologies sont proposés qui peuvent modifier notre vie privée ou nos attentes face à ce sujet. Compte tenu de leur potentiel d'impact sur la société canadienne, il y a du bon sur les plans politique, commercial et social à évaluer ces propositions avant de les mettre en application. Les études d'impact environnemental font régulièrement partie de l'examen de nombre de nouvelles propositions et s'en sont révélées des composantes essentielles. Les nouveaux progrès technologiques font de la protection de la vie privée un enjeu aussi important en ce début de siècle que l'était la protection environnementale à la fin du dernier. Les études d'impact sur la vie privée ont désormais acquis leurs lettres de noblesse.

Ces études sont menées à des fins nombreuses :

- Elles permettent de sonner rapidement l'alarme et font office d'outil de planification précoce ;
- Elles permettent d'éviter les lacunes des nouvelles propositions, empêchant la mauvaise presse, la perte de la crédibilité et de la confiance du public — sans oublier les coûts, les correctifs et les sanctions juridiques possibles ;
- Elles prévoient et (ou) confirment les impacts qu'auront les propositions sur la vie privée des individus ou de groupes ;
- Elles évaluent dans quelle mesure une proposition est conforme aux lois et aux principes régissant la vie privée ;
- Elles déterminent les interventions et les stratégies correctives nécessaires pour éviter ou surmonter tout impact négatif ; et
- Elles sensibilisent davantage les Canadien(ne)s aux enjeux de vie privée, les informent des détails de la proposition et les font participer à sa conception, à son acceptation et à sa mise en œuvre.

Le processus

Qui ? La partie la mieux placée pour mener une étude d'impact sur la vie privée devrait être l'organisme du secteur public ou privé qui pilote la proposition. Même si les commissaires à la vie privée ou à la protection des renseignements personnels s'y connaissent dans ce domaine, personne ne connaît mieux les détails que les personnes qui ont conçu le produit ou le service proposé. Elles sont les mieux placées pour répondre aux questions que soulève l'étude d'impact. Toutefois, pour garantir l'objectivité de cette

dernière, l'organisation devrait consulter les Canadien(ne)s concerné(e)s, soumettre l'étude d'impact une fois terminée à l'examen d'un expert en vie privée indépendant et mettre l'étude d'impact à la disposition du public.

Quand ? Selon toute logique, l'étude d'impact devrait faire partie de la phase de conception de la proposition et être entreprise aussitôt que l'organisation décide d'examiner sa faisabilité. Même si certaines études d'impact peuvent être terminées avant la mise en œuvre de la proposition, d'autres peuvent se poursuivre pendant sa mise en œuvre. D'autres encore sont sans fin et deviennent partie intégrante d'un processus continu de contrôle de la qualité.

Quoi ? Même si chaque étude d'impact varie selon la nature et les circonstances entourant chaque proposition, toutes les propositions doivent être évaluées en fonction de principes de gestion des renseignements personnels acceptés à l'échelle internationale, des lois pertinentes sur la vie privée ainsi que des attentes des Canadien(ne)s concerné(e)s face à leur vie privée.

Comment ? Chaque étude d'impact doit aborder et documenter les éléments suivants :

Proposition : L'organisation doit décrire la proposition de façon approfondie, fournir des détails sur ses composantes et l'échéancier, présenter des informations de fond et faire état de la portée de la proposition (qui sera touché, et de quelle façon ?);

Impacts : L'organisation doit ensuite décrire les incidences positives et négatives (connues et prévues) que la proposition aura sur la vie privée des Canadien(ne)s. L'organisation doit décrire la nature cumulative de chaque impact ainsi que sa durée, sa fréquence, son intensité, sa probabilité et sa portée, puis elle doit en évaluer l'intensité (faible, moyenne ou élevée) ;

Nécessité : L'organisation doit justifier la nécessité (autre que le bénéfice commercial) de la proposition proprement dite, le moment où elle est présentée et ses impacts négatifs ;

Conformité : L'organisation doit évaluer sa proposition en fonction des principes internationaux susmentionnés de gestion des renseignements personnels, des lois pertinentes sur la vie privée ainsi que des attentes des Canadien(ne)s concerné(e)s face à leur vie privée ;

Alternatives et solutions : L'organisation doit déterminer tout alternative qui permettrait d'éviter les impacts et les problèmes de conformité identifiés

ci-dessus ainsi que les solutions qui permettraient d'éliminer ou d'atténuer un impact ou un problème de conformité donné.

Le Commissariat fédéral à la protection de la vie privée effectue certaines études d'impact sur la vie privée soit à la demande expresse de certains organismes des secteurs public ou privé ou de son propre chef (pour mieux comprendre les détails et les répercussions d'une technologie ou d'un projet donné). Pour obtenir de plus amples renseignements au sujet des études d'impact sur la vie privée, une liste des principes de gestion des renseignements personnels ou des lois pertinentes sur la vie privée, veuillez communiquer avec nous ou visiter notre site Web.

Partage des données à l'Agence des douanes et du revenu du Canada (ADRC)

Au début de 1995, le Commissariat a passé en revue toutes les institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels* afin d'établir dans quelle mesure elles partageaient ou couplaient officiellement ou officieusement des renseignements personnels. Parmi celles qui ont déclaré partager des renseignements personnels, Revenu Canada (aujourd'hui devenu l'Agence des douanes et du revenu du Canada) a reconnu partager divers renseignements sur ses clients avec d'autres institutions fédérales, provinciales et étrangères pour les aider à gérer leurs programmes d'une façon plus efficace et plus économique. Le partage de l'information vise principalement à éviter de recueillir des renseignements sur des personnes, des entreprises ou des organismes qui sont déjà accessibles dans une autre institution ou dans un autre ordre de gouvernement. L'information communiquée par Revenu Canada allait de l'ensemble de ses dossiers de contribuables sous forme électronique à quelques renseignements sur copie papier.

Le Ministère a annexé à ses réponses au sondage une liste de plus de 200 ententes écrites conclues avec d'autres institutions gouvernementales, ainsi qu'une description générale des objectifs visés par ces ententes et leur fondement juridique. Selon le Ministère, toutes ces ententes étaient conformes aux lois administrées par ses fonctionnaires (soient la *Loi de l'impôt sur le revenu*, la *Loi sur la taxe d'accise*, la *Loi sur les douanes*, etc.), conformes aux dispositions de *la Loi sur la protection des renseignements personnels*, et inscrites dans le catalogue *InfoSource*.

Le nombre d'ententes de partage conclues par Revenu Canada s'est considérablement accru depuis 1995. Selon l'ADRC, il existe maintenant plus

de 300 ententes écrites d'échange de renseignements personnels avec des organismes extérieurs. Il semble que cette augmentation rapide soit attribuable à une plus forte pression visant à offrir des services plus efficients et efficaces, de même qu'à la nouvelle orientation de l'Agence en tant que gestionnaire de prestations pour des partenaires extérieurs.

Étant donné le nombre important d'ententes, la portée de leurs objectifs et les partenaires visés, le Commissariat a avisé l'ADRC en décembre dernier de son intention de réviser ces ententes de partage de façon informelle. Il s'agira d'établir jusqu'à quel point les échanges d'information sont conformes aux dispositions de la *Loi sur la protection des renseignements personnels*. Une attention particulière sera prêtée aux ententes conclues avant l'entrée en vigueur de cette dernière. Notre révision déterminera également si certaines des ententes de partage constituent en fait un couplage de données aux termes de la politique du Conseil du Trésor à ce sujet. Cette politique exige notamment que le Commissaire à la protection de la vie privée soit prévenu de tout nouveau couplage de données.

L'ADRC a assuré le Commissariat de son entière collaboration pendant sa révision.

Sondages de la clientèle

L'an dernier, le Commissariat a reçu plusieurs demandes de renseignements de la part d'institutions fédérales qui envisageaient de recourir aux services de firmes de sondage privées pour la conduite de sondages sur la satisfaction de la clientèle. Toutes voulaient savoir si le fait de communiquer des renseignements personnels sur le client à la firme de sondage constituait une infraction à la *Loi sur la protection des renseignements personnels*.

Dans chaque cas, nous savions pertinemment que les seules raisons pour lesquelles les ministères voulaient mener un sondage étaient d'évaluer la satisfaction de leurs clients à l'égard des services et de déterminer comment améliorer ces derniers. Nous reconnaissons qu'il est raisonnable pour les organismes publics d'avoir certains rapports avec leurs clients pour améliorer le service à la clientèle, mais quel qu'en soit le besoin, une institution doit satisfaire à trois exigences importantes avant de communiquer des renseignements personnels sur ses clients à une firme de sondage externe. Voici ces exigences :

Autorisation de recueillir des renseignements personnels — Avant de recueillir les renseignements aux fins du sondage, l'institution doit s'assurer

qu'elle y est autorisée par la loi. Cela signifie que le sondage doit être directement lié aux programmes ou aux activités de l'institution.

Autorisation de communiquer des renseignements personnels — Le fait qu'une institution gouvernementale soit autorisée à recueillir des renseignements personnels sur le client ne signifie pas nécessairement qu'elle est autorisée à communiquer les renseignements à une organisation externe afin que celle-ci mène un sondage. Certaines lois définissant et limitant expressément les circonstances permettant la communication de renseignements personnels, l'institution doit donc s'assurer que sa loi habilitante ne l'empêche pas de communiquer des renseignements personnels à une firme de sondage privée.

Conformité avec la *Loi sur la protection des renseignements personnels* — si l'on tient pour acquis que les propres lois de l'institution ne l'empêchent pas de communiquer des renseignements, l'institution doit s'assurer que la communication des renseignements personnels est conforme à la *Loi sur la protection des renseignements personnels*. Cette Loi ne permet la communication de renseignements personnels de clients à des fins de sondages externes que si a) les personnes concernées sont informées au moment de la collecte que leurs renseignements pourraient être utilisés ou communiqués à cette fin, b) les personnes ont consenti à ce que leurs renseignements soient utilisés ou communiqués à cette fin, et c) la divulgation est permise en vertu du paragraphe 8(2) de la Loi.

Dans certaines circonstances, l'alinéa 8(2)a) pourrait être utilisé pour justifier la communication des renseignements à une firme de sondage, mais seulement si le sondage est suffisamment pertinent au programme qu'il en devienne une utilisation conforme des renseignements selon l'alinéa 7(a) de la Loi.

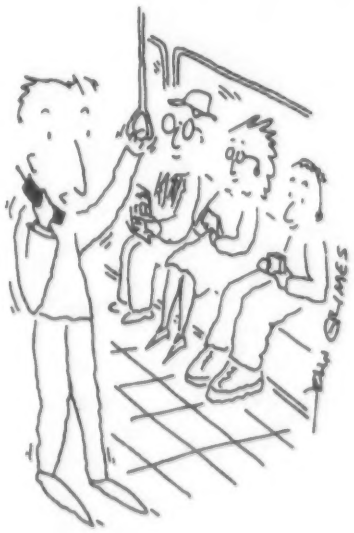
La Loi ne définit pas l'expression « usage compatible » aux fins de ces articles. Cependant, les lignes directrices du Conseil du Trésor sur l'administration de la *Loi sur la protection des renseignements personnels* stipulent que, « pour qu'un usage (…) soit compatible, il doit y avoir un lien pertinent et direct avec les fins premières pour lesquelles ces renseignements ont été recueillis ou consignés ». De plus, il y est dit que « les fins premières et les fins prévues sont si intimement liées que la personne s'attend à ce que les renseignements soient utilisés à une fin compatible, même si l'usage n'est pas expressément indiqué ». Pour déterminer si l'usage est bel et bien compatible, il faut analyser deux éléments : un élément objectif (le lien pertinent et direct avec les fins premières pour lesquelles ces renseignements ont été recueillis) et un

élément subjectif (une personne raisonnable s'attend à ce que l'institution utilise les renseignements de cette façon).

Puisqu'il est difficile d'évaluer les attentes raisonnables d'un client, les ministères devraient se rabattre sur la notion d'utilisation conforme s'ils songent à communiquer des renseignements personnels à des maisons de sondage dans des circonstances exceptionnelles. Cela constitue cependant la façon la moins souhaitable de communiquer les renseignements de personnes dont le gouvernement souhaite la coopération. Ces gens n'en savent rien au départ, et s'irritent souvent de recevoir des appels de maisons de sondage. Il est nettement préférable d'obtenir le consentement préalable de ces personnes.

Nous encourageons chaque organisme fédéral à tout mettre en œuvre pour prévenir ses clients sans délai de la possibilité qu'une maison de sondage les contacte. Chaque organisme devrait également indiquer à ses clients les dispositions juridiques permettant de tels sondages, les objectifs visés, les utilisations prévues pour les résultats et la raison pour laquelle certains clients ont été retenus pour être sondés. Ces clients devraient également apprendre que leur participation aux sondages est facultative, qu'ils peuvent interdire la communication de leurs renseignements personnels, et qu'ils peuvent refuser de participer à tout sondage à l'avenir.

Si un sondage doit se répéter sur une base régulière, l'organisme doit en aviser ses clients lors de la collecte de leurs renseignements et doit obtenir leur consentement préalable. Le sondage doit aussi être décrit sous le fichier approprié du catalogue *InfoSource*.



"ET SURTOUTNE SOUFFLEZ MOT DE CECI À PERSONNE."

Quoique le recours à une maison de sondage externe ne contrevienne pas à la *Loi sur la protection des renseignements personnels*, l'organisme fédéral doit prendre toutes les mesures nécessaires afin de réduire les atteintes à la vie privée qui résulteraient d'un tel recours. Par exemple, l'organisme ne devrait communiquer à la maison de sondage que ceux des renseignements personnels essentiels à l'échantillonnage et au

sondage des personnes visées. Idéalement, l'organisme minimiserait encore davantage les atteintes à la vie privée de ses clients en effectuant lui-même leur échantillonnage.

Si cette situation idéale s'avère impossible ou peu pratique, l'organisme devrait songer à remettre à la maison de sondage une liste dépersonnalisée de l'ensemble de ses clients, à partir de laquelle sera construit l'échantillon. Une fois le nombre requis de clients retenu, l'organisme pourra alors en révéler l'identité à la maison de sondage.

Les institutions fédérales sont responsables de la protection des renseignements personnels de leurs clients pendant un sondage. Le contrat passé avec la maison externe devrait stipuler que ces renseignements personnels demeurent sous le contrôle de l'institution fédérale et assujettis aux dispositions de la *Loi sur la protection des renseignements personnels*. Le contrat devrait également clairement traiter de l'usage, de la collecte, de la communication, de la protection, de la sécurité et de la destruction de tout renseignement personnel recueilli par la maison dans le cadre du contrat. Ce dernier devrait notamment exiger de la maison de sondage qu'elle :

- informe chaque client en début d'entretien : du fait que ses renseignements sont recueillis au nom de l'institution fédérale partie au contrat ; de l'objectif de la collecte et de l'usage prévu des résultats du sondage ; du fait que les réponses du client seront dépersonnalisées avant d'être remise à l'institution fédérale, à moins que le client ne permette clairement le contraire ; que la participation du client est facultative et que tout refus de participer n'affectera en rien l'accès par le client aux services et programmes de l'institution fédérale en question ;
- détruise, une fois les réponses compilées, l'élément lui permettant de relier l'identité d'un client donné à ses réponses ;
- se débarrasse, une fois le sondage terminé et conformément à la *Loi sur la protection des renseignements personnels*, de tous les renseignements reçus de l'institution fédérale partie au contrat, et renvoie à cette institution tous les renseignements, dépersonnalisés, obtenus lors du sondage.

Avant d'entreprendre un sondage, un organisme fédéral doit évaluer l'impact d'un tel sondage sur la vie privée de ses clients. Les sondages ne sont pas obligatoirement le meilleur outil de mesure de la qualité d'un service ou de l'efficacité de certaines politiques ou activités. L'organisme fédéral devrait d'abord se tourner vers d'autres sources d'information, ce qui pourrait lui éviter de devoir communiquer des renseignements personnels à des tiers.

Centre et Registre canadiens des armes à feu — Ministère de la Justice du Canada

Par le passé, certains rapports annuels ont fait ressortir les enjeux pour la vie privée inhérents à la création, par le gouvernement, du Registre canadien des armes à feu. Le personnel du Commissariat a passé beaucoup de temps à examiner le programme et ses répercussions sur la vie privée. Même si certains progrès ont été accomplis, il reste des problèmes à régler en ce qui a trait à différentes compétences et aux droits (et moyens) de chacun d'accéder à ses renseignements personnels dans le registre. De plus, les nombreux partenaires qui entrent en jeu, le manque d'homogénéité opérationnelle d'une province à une autre et la complexité des connections physiques et technologiques de ce programme ont soulevé des questions quant à la quantité et au détail des renseignements personnels dont ont besoin les préposés aux armes à feu pour remplir leurs obligations en vertu de la *Loi sur les armes à feu.*

En janvier 2000, le Commissaire à la protection de la vie privée a entrepris d'évaluer de façon approfondie les pratiques de gestion des renseignements personnels des employés du Registre canadien des armes à feu. Cet examen comprendra des visites tant du bureau central de traitement à Miramichi (N.-B.) que des bureaux du Contrôleur fédéral et de certains Contrôleurs provinciaux des armes à feu, ainsi que du Centre et du Registre canadiens des armes à feu, dans la région de la capitale nationale. Le Commissaire entreprend cet examen dans l'optique de pouvoir régler au moins toutes les questions et les plaintes qu'il a reçues jusqu'ici. Le sous-ministre de la Justice a accueilli l'annonce de l'examen avec plaisir, et s'est dit intéressé par toute observation et recommandation qui aiderait le Centre canadien des armes à feu à satisfaire aux exigences prévues par la *Loi sur la protection des renseignements personnels.*

Couplages avec les dossiers de Prestation fiscale pour enfants

Ce qui était proposé — En août 1998, l'Agence des douanes et du revenu du Canada (ADRC) a dit au Commissaire à la protection de la vie privée qu'elle comptait coupler la liste des familles touchant la prestation fiscale canadienne pour enfants (PFCE) avec celle de tous les décès enregistrés par les organismes provinciaux responsables de l'état civil. Ensuite, en octobre 1998, le Commissaire a été avisé d'un deuxième couplage de la même liste, cette fois-ci avec toutes les nouvelles naissances enregistrées. Les couplages visaient à identifier les familles qui réclament la PFCE, mais qui n'y sont pas

admissibles, et celles qui ne la réclament pas, mais y sont admissibles.

Ces deux propositions ont été provoquées par le rapport de 1996 du Vérificateur général, qui a révélé que le programme de la PFCE manque de mécanismes fondamentaux de vérification. Le Vérificateur général a fait remarquer que l'ADRC devait trouver de meilleures façons de servir les familles à faible revenu, à l'aide des nouvelles technologies et en forgeant des partenariats avec les provinces.

Contexte — La PFCE est un paiement mensuel exempt d'impôt qui aide les familles admissibles à élever leurs enfants de moins de 18 ans. La PFCE s'assortit du Supplément de la prestation nationale pour enfants, prestation offerte conjointement par les gouvernements fédéral, provinciaux et territoriaux aux familles à faible revenu. L'ADRC utilise les renseignements recueillis sur les formulaires de demande de la PFCE pour administrer les deux programmes, ainsi que plusieurs programmes provinciaux et territoriaux de prestation pour enfants et de crédits d'impôt.

En juillet, lorsqu'elle reçoit les déclarations de revenus des parents sur lesquelles figurent le revenu net total, l'ADRC recalcule automatiquement les prestations pour la période allant de juillet à juin. Si l'enfant est né à l'extérieur du Canada ou s'il est né au Canada et a au moins un an, ses parents doivent fournir une preuve de naissance. Pour recalculer l'admissibilité, l'ADRC doit être avisée de tout changement relatif à la garde de l'enfant (notamment le décès de l'enfant), à l'état civil, aux nouvelles cotisations de l'impôt, au statut de citoyenneté ou d'immigration, et à l'adresse (à moins que les prestations ne soient déposées directement dans le compte).

Même si le Commissaire à la protection de la vie privée ne met pas en doute que le fait de recueillir des statistiques provinciales de l'état civil puisse aider l'ADRC à administrer le programme de prestations fiscales, il faudra régler plusieurs questions avant qu'il ne souscrive à l'échange d'informations. Le problème de base de tout couplage de données est qu'il suppose l'usage de renseignements personnels à l'insu et sans le consentement de la personne concernée, et à des fins autres que celles pour lesquelles ils ont été recueillis. Cela est contraire à l'esprit des pratiques équitables de gestion de l'information prévues dans la *Loi sur la protection des renseignements personnels*. L'échange d'informations entre les organismes provinciaux responsables des statistiques de l'état civil et l'ADRC soulève également des préoccupations quant à la confidentialité et à la sécurité de l'information.

Même si le couplage des données contenues dans le registre des décès révèle

une perte de revenus apparente, parce que 25 p. 100 des parents n'avisent pas l'ADRC d'un décès, ce couplage de données soulève des préoccupations importantes sur le plan de la vie privée et pourrait entraîner de graves allégations selon lesquels certains parents profitent frauduleusement du décès de leur enfant. De plus, le Commissaire à la protection de la vie privée n'est pas convaincu que la vie privée des cinq pour cent de parents ne réclamant pas de PFCE mérite l'atteinte que représente le recours au registre des naissances, surtout que l'institution a déjà mis en place un très bon programme de sensibilisation publique.

Le Commissariat a fait parvenir ses commentaires préliminaires à l'ADRC au début de décembre 2000, et n'en a pas encore reçu de réponse.

Disparition d'un ordinateur portatif à Halifax — Service correctionnel du Canada

En janvier 1999, un individu est entré par effraction dans le Bureau sectoriel de libérations conditionnelle de Halifax du Service correctionnel du Canada. Il a volé un ordinateur portatif, une veste et un trousseau de clés appartenant à un employé contractuel. Le SCC a alors convoqué un Comité d'enquête, l'ordinateur portatif contenant en effet des données psychologiques sur près de 130 contrevenants (tous ont été avisés). Voici les résultats du rapport d'enquête :

- Les données contenues dans l'ordinateur portatif comportaient les résultats d'un examen psychologique auto-administré et un profil incluant le nom, l'âge, le numéro du Service canadien des pénitenciers, les condamnations les plus récentes, la liste d'examens subis et une interprétation de leurs résultats, et ce pour chacun des 130 contrevenants en question ;
- Les contrevenants se servaient beaucoup de l'ordinateur portatif et connaissaient son emplacement ;
- Le bureau utilisé donnait accès à une sortie de secours menant à une zone commune, à un ascenseur et à un escalier, et la plupart des contrevenants avaient remarqué que n'importe qui pouvait sortir rapidement du bureau en passant par la porte non verrouillée ;
- N'importe quel contrevenant ou employé pouvait accéder au contenu de l'ordinateur portatif, auquel était relié un modem communiquant avec l'Internet ;
- L'ordinateur portatif contenait des renseignements personnels confidentiels et était souvent laissé sans surveillance. Quelquefois, les

aussi étaient laissés sans surveillance ;

- SCC n'avait pas mis à jour les procédures et les politiques relatives à la sécurité du bureau depuis un certain temps. Les employés ne connaissaient pas bien les exigences en matière de sécurité, et la sécurité globale physique et informatique laissait à désirer.

Le rapport du Comité d'enquête a mené à une refonte complète des procédures de sécurité. Le SCC a pris plusieurs autres mesures, notamment :

- faire des politiques de sécurité un sujet permanent de discussion dans les réunions de district ;
- inclure un volet de sensibilisation à la sécurité à ses séances d'information et d'acquisition de compétences en cours d'emploi ;
- utiliser un seul ordinateur portatif (qui appartient au SCC, et non à un sous-traitant) pour l'administration des auto-examens psychologiques des contrevenants. Le personnel utilisera un autre ordinateur pour préparer des rapports sommaires ;
- transférer l'information sur une disquette pour préparer un rapport et effacer toutes les données du disque dur de l'ordinateur portatif chaque fois qu'un contrevenant termine l'examen ;
- accompagner les contrevenants en tout temps, même pendant l'examen. À leur arrivée, tous les visiteurs et tous les contrevenants doivent s'inscrire à la réception. Ils ne peuvent entrer directement dans l'aire de travail ;
- retirer le modem de l'ordinateur portatif, ce qui empêche les contrevenants d'accéder au Système de gestion des détenus, au système de courrier électronique du SCC ou à l'Internet ;
- installer une serrure sur la porte de secours afin d'empêcher les gens d'entrer de l'extérieur.

Malheureusement, on n'a jamais retrouvé l'ordinateur portatif. Il n'y a aucune façon de savoir ce que le voleur a fait des renseignements (s'il les a utilisés) ou si le voleur était intéressé par le contenu de l'ordinateur. Si l'ordinateur portatif a été vendu, espérons que son contenu a été effacé. Évidemment, le Bureau sectoriel de libération conditionnelle de Halifax n'a pas su manipuler et protéger adéquatement les renseignements personnels confidentiels, mais le Commissaire à la protection de la vie privée est satisfait des mesures correctives qu'a prises le SCC.

Communication dans l'intérêt public — Renseignements médicaux d'un membre décédé des Forces canadiennes

Le ministère de la Défense nationale a proposé, pour aider la veuve d'un membre des Forces canadiennes à régler une réclamation d'assurance vie, la divulgation à la compagnie d'assurances concernée d'une copie des deux dernières années du dossier médical du défunt militaire.

Le personnel du Commissaire à la protection de la vie privée a contesté le besoin de divulguer le dossier médical, dont la plupart des pages n'avaient aucun rapport avec la situation médicale en cause. De plus, comme les renseignements médicaux devaient être séparés d'autres données de nature délicate, la compagnie d'assurances était peu susceptible de se satisfaire de documents partiels, s'interrogeant sur ce qui avait été retiré du dossier. La réclamation risquait donc de demeurer insuffisamment justifiée.

Suite à des discussions avec le personnel du Commissaire à la protection de la vie privée, la Défense nationale a accepté de ne fournir à la compagnie d'assurances que les renseignements pertinents. Le Directeur, Politique de santé du MDN, a écrit à la compagnie d'assurances pour confirmer que le militaire n'avait pas souffert de la maladie visée par la réclamation.

Le Commissaire à la protection de la vie privée s'est dit satisfait. Même si la lettre à la compagnie d'assurances divulguait des renseignements personnels, l'invasion de la vie privée du défunt avait été réduite de beaucoup. Tout en ne divulguant aucun dossier spécifique des registres médicaux militaires, la Défense nationale avait pu répondre aux exigences de la compagnie d'assurances. Cette communication de renseignements personnels pour des raisons d'intérêt public a été faite pour un motif humanitaire.

Un respect trop littéral de la Loi : rapports annuels des institutions fédérales

Le Commissaire à la protection de la vie privée se préoccupe de plus en plus de la façon dont les institutions fédérales préparent leur rapport annuel sur leurs activités en vertu de la *Loi sur la protection des enseignements personnels*. Comme le prévoit l'article 72 de la Loi, l'original de ces rapports est soumis au Parlement et une copie au Commissaire. Ce dernier en prend fidèlement connaissance, année après année, mais a l'impression grandissante qu'il y manque quelque chose de fondamental. Non pas un manque de conformité à la Loi, que ces rapports respectent en tous points. Mais la Loi exige si peu en partant. Vu l'importance tant des enjeux entourant notre vie privée que des

lecteurs de ces rapports (les parlementaires), le Commissaire est de plus en plus d'avis que les institutions fédérales assujetties à la *Loi sur la protection des renseignements personnels* peuvent, et doivent, faire mieux.

À quelques exceptions remarquables, ces rapports ne fournissent pas au lecteur une vue d'ensemble des enjeux de vie privée au sein de l'organisme. Un rapport type comprend un rapport statistique et un énoncé descriptif. Le rapport statistique est un tableau d'une page indiquant le nombre de demandes reçues en vertu de la Loi et comment ces dernières sont traitées, le nombre de plaintes déposées auprès du Commissaire et les conclusions de ce dernier, et les coûts reliés à l'application de la Loi. L'énoncé quant à lui comporte une description de l'institution et de son mandat, et de la façon dont elle applique la *Loi sur la protection des renseignements personnels* — qui est responsable de quoi et qui se rapporte à qui — deux éléments qui changent peu d'année en année. Le reste de l'énoncé se limite souvent à répéter en phrases les chiffres du rapport statistique.

Ces rapports s'adressent au Parlement. Les députés et sénateurs n'ont pas besoin de connaître les détails de l'application de la Loi au sein d'une institution donnée lorsqu'ils étudient les programmes et les dépenses de cette dernière. Ce qu'ils ont besoin de savoir, par contre, sont les deux grandes questions ayant des incidences sur la vie privée : ententes de couplages de données et impacts de projets de loi sur la vie privée. Nos parlementaires veulent en apprendre davantage sur les incidences d'une nouvelle technologie, politique ou pratique sur la vie privée, surtout dans le contexte d'une fonction publique en rapide évolution.

Les institutions fédérales doivent concentrer leurs efforts sur ces questions pour être à même d'en traiter dans leur rapport annuel. Et ce dernier devrait être leur principal incitatif. Se sachant obligées de préparer un rapport sérieux sur la question, ces institutions pourraient ainsi commencer à faire ce que le Commissariat préconise depuis longtemps : mener des études d'impact de leurs politiques et programmes sur la vie privée. Ce faisant, nous les invitons à consulter le Commissariat, tout comme l'ont fait le Directeur général des élections quant au registre permanent des électeurs, et Développement des ressources humaines Canada quant à l'idée d'un numéro national d'identification de la clientèle.

Nos inquiétudes quant à l'état actuel de ces rapports annuels ne doivent surtout pas être perçues comme une critique des employés qui consacrent beaucoup d'efforts à les préparer. Ces professionnels chargés de l'application de la *Loi sur la protection des renseignements personnels* au sein des institutions fédérales sont les piliers de la Loi et ses protecteurs quotidiens. Mais des

rapports plus élaborés sur les vrais enjeux pour la vie privée capteraient mieux l'attention des parlementaires, et conféreraient à ces professionnels la reconnaissance professionnelle et l'importance qu'ils méritent.

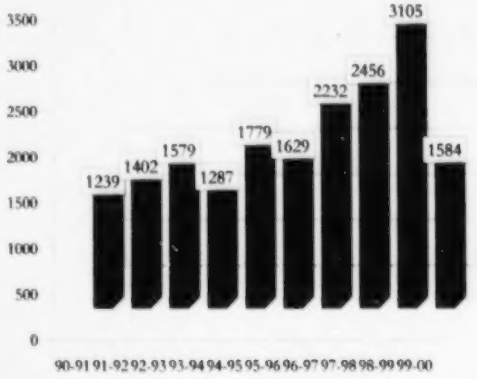
Le Commissaire à la protection de la vie privée encourage le Conseil du Trésor — chargé de l'administration de la *Loi sur la protection des renseignements personnels* — à se pencher sur la meilleure façon de rendre ces rapports annuels plus importants et utiles.

Direction des enquêtes et demandes de renseignements

Après les hausses remarquables des trois dernières années, le nombre de plaintes déposées cette année a chuté à un niveau sans précédent depuis la moitié de la décennie. En 1999-2000, le Commissariat a reçu 1 584 plaintes. On est bien loin du record de 3 105 plaintes enregistré en 1998-1999.

Plaintes reçues

par exercice financier



Cette diminution est en grande partie attribuable au déclin marqué du nombre de plaintes visant le couplage par le gouvernement entre les déclarations de douane des voyageurs et les demandes d'assurance emploi. La cause était en effet devant les tribunaux. Cette année, le Commissariat n'a reçu que 27 plaintes de ce genre par rapport à 1 327 en 1998-1999 et 963 en 1997-1998.

Un autre facteur important qui a mené au record enregistré l'an dernier est le fait que, en 1998, le personnel des Services correctionnels du Canada ait déposé 225 plaintes de délai dans le cadre d'un conflit de travail. De même, en 1996-1997, trois personnes avaient déposé plus de la moitié des 1 065 plaintes de délai que nous avions reçues. Cette année, le Commissariat n'a pas reçu autant de plaintes provenant d'un seul organisme ou d'un petit nombre de personnes.

Contrairement aux chiffres des deux exercices précédents, le nombre total de plaintes reçues en 1999-2000, ainsi que leur ventilation par type, s'apparente aux tendances projetées en fonction des initiatives entreprises par le Commissariat à la protection de la vie privée et les ministères fédéraux. De façon plus spécifique, les efforts que le Commissariat a déployés envers les ministères les plus souvent visés par des plaintes de délai semblent finalement

avoir porté fruit : le nombre total de ces plaintes a presque diminué de moitié cette année.

Le personnel du Commissariat à la protection de la vie privée a mené 1 399 enquêtes, dont 582 ont conclu au bien-fondé de la plainte. Trois cent quarante-sept plaintes se sont avérées non fondées, 82 fondées et résolues, 34 résolues et 282 réglées en cours d'enquête. Les 72 autres plaintes ont été abandonnées pour diverses raisons. (voir l'explication de ces catégories plus bas.)

Enquêtes réglées par motifs et résultats

pour l'exercice financier prenant fin le 31 mars 2000

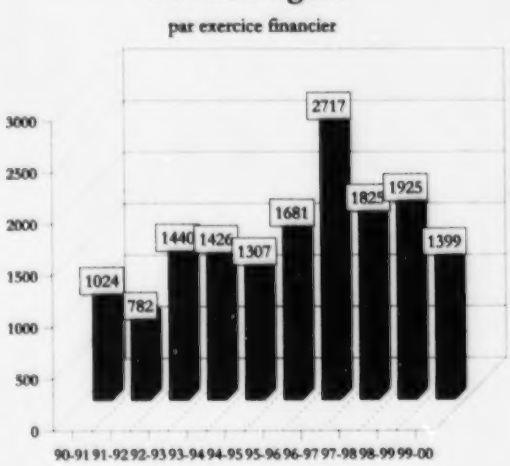
	Fondée	Fondée; résolue	Non fondée	Aban-donnée	Résolue	Réglée	Total
Accès	**15**	**68**	**172**	**33**	**31**	**184**	**503**
Accès	14	67	170	32	29	177	489
Correction/Annotation	1	1	2	1	2	6	13
Langue	0	0	0	0	0	1	1
Atteinte à la vie privée	**73**	**13**	**113**	**28**	**3**	**81**	**311**
Collecte	0	2	34	7	1	19	63
Conservation/Retrait	5	0	4	2	0	7	18
Usage/Communication	68	11	75	19	2	55	230
Délais	**494**	**1**	**61**	**11**	**0**	**17**	**584**
Correction/Délais	25	0	3	0	0	0	28
Délais	466	1	33	11	0	11	522
Avis de prorogation	3	0	25	0	0	6	34
Autres	**0**	**0**	**1**	**0**	**0**	**0**	**1**
Autres	0	0	1	0	0	0	1
Total	**582**	**82**	**347**	**72**	**34**	**282**	**1399**

Pendant le mandat du Commissaire

Le Commissaire Phillips a vu le nombre de plaintes reçues annuellement passer de 1 239 en 1990-1991, à 3 105, en 1998-1999. À l'exception du total exceptionnellement bas de cette année, le nombre de plaintes reçues a augmenté en moyenne de plus de 10 p. 100 par année au cours du mandat du Commissaire, lequel a traité un total de 15 526 plaintes.

Les tableaux précédents indiquent le nombre total de plaintes reçues et examinées pour chacune des dix années que le Commissaire a passées à son poste.

Au fil des ans, le Commissaire a également assisté à un changement important des types de plaintes reçues. En moyenne, le nombre de plaintes de délai a diminué, et celui des plaintes liées à la gestion des renseignements personnels a augmenté en proportion du total. L'importance de cette tendance est attribuable au fait que les deux types de plaintes ne présentent pas la même complexité.



Habituellement, il est plus facile et plus rapide d'étudier les plaintes de délai étant donné qu'elles n'exigent en général qu'un appel téléphonique ou une lettre. Par contre, les plaintes relatives à la gestion des renseignements personnels ont tendance à être beaucoup plus complexes et prenantes et exigent des visites sur place (souvent dans des bureaux régionaux éloignés), de nombreux entretiens avec le personnel du ministère concerné, des examens approfondis des dossiers et un rapport détaillé des résultats. L'accroissement relatif du nombre de plaintes liées à la gestion des renseignements personnels semble également avoir fait augmenter la durée moyenne de nos enquêtes, ainsi que la charge de travail de nos enquêteurs.

Au fil des ans, le Commissaire a également remarqué un changement considérable de la nature des plaintes découlant de refus d'accès. Nos enquêtes consistaient habituellement en un simple examen des documents refusés. Aujourd'hui, toutefois, de nombreuses plaintes de refus d'accès supposent qu'il faut tenir compte de documents manquants. En outre, ces plaintes visent de plus en plus des dossiers non officiels dont l'organisme refuse souvent d'admettre l'existence, compliquant d'autant notre enquête.

De plus, tant les plaignants que les représentants de l'AIPRP des ministères semblent avoir amélioré leurs connaissances et leur recours aux exceptions au

droit d'accès. En conséquence, les discussions concernant la validité des refus d'accès sont devenues plus complexes, augmentant d'autant la durée moyenne de nos enquêtes et la charge de travail de notre personnel.

En tout et pour tout, en dix années de service, le Commissaire a constaté que les plaintes devenaient plus exigeantes et les enquêtes, plus difficiles.

Définitions des conclusions possibles de nos enquêtes

Pour conclure l'étude d'une plainte, le Commissaire à la protection de la vie privée utilise l'une des six expressions suivantes, qui indiquent sa conclusion :

- plainte non fondée ;
- plainte fondée ;
- plainte fondée/résolue ;
- plainte résolue ;
- plainte réglée en cours d'enquête ;
- plainte abandonnée.

Voici les définitions de ces expressions. Elles vous permettront de mieux les distinguer.

Plainte non fondée
Lorsqu'on indique que la plainte n'est pas fondée, cela signifie que l'enquête n'a relevé aucune preuve qui pourrait amener le Commissaire à la protection de la vie privée à conclure que l'institution fédérale a violé les droits que la *Loi sur la protection des renseignements personnels* confère au plaignant. Par exemple, le Commissaire pourrait arriver à cette conclusion lorsque :

- dans le cas d'une plainte relative à une interdiction d'accès, toutes les informations pertinentes à la demande d'accès ont été traitées ou que les raisons invoquées par l'institution fédérale pour refuser l'accès étaient justifiées ;
- dans le cas d'une plainte relative à une communication abusive, le Commissaire à la protection de la vie privée s'est fondé sur les preuves recueillies au cours de l'enquête et sur les observations de l'institution fédérale pour décréter que la communication des renseignements personnels satisfaisait aux exigences prévues au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

Plainte fondée

Lorsqu'on conclut qu'une plainte est fondée, cela signifie que l'institution fédérale n'a pas respecté les droits d'une personne qui lui sont conférés par la *Loi sur la protection des renseignements personnels*, et qu'aucune mesure corrective n'aurait pu atténuer la violation de la vie privée. En d'autres termes, même si l'institution fédérale est fautive, ce qui est fait est fait, et l'on ne peut rien changer à la situation. Le Commissaire arrive habituellement à ce genre de conclusion dans les cas où l'institution a utilisé ou communiqué des renseignements personnels de façon abusive ou n'a pas répondu à une demande d'accès dans les délais prescrits par la Loi. Cette conclusion serait aussi celle retenue dans les cas où une institution fédérale refuse de communiquer des renseignements malgré la recommandation du Commissaire, lequel refus pourrait mener à une demande de révision par la Cour fédérale du Canada.

Plainte fondée/résolue

On conclut que la plainte est fondée/résolue lorsque des allégations portées dans le cadre de la plainte sont corroborées par l'enquête, mais que l'institution fédérale a déjà accepté de prendre des mesures correctives pour régler le problème. Le Commissaire arrive à ce résultat lorsque, par exemple, un ministère :

- accepte de fournir au plaignant les renseignements auxquels il n'avait pas accès auparavant ;
- entreprend d'améliorer une politique ou une pratique pour respecter la *Loi sur la protection des renseignements personnels.*

Plainte résolue

La catégorie des plaintes résolues reconnaît la nécessité d'arriver à un règlement conforme au rôle de l'ombudsman, lequel consiste à régler les plaintes en faisant preuve de souplesse. Avant 1994, le Commissaire ne savait trop comment considérer certaines plaintes qu'il ne pouvait pas vraiment qualifier de « fondées » parce que, pour l'essentiel, il y avait eu une mauvaise communication ou un malentendu.

Exemples de plaintes résolues :

- Il y a eu une mauvaise communication ou un malentendu entre le plaignant et l'institution fédérale concernant l'information demandée. Les deux parties ont accepté une solution qui les satisfaisait mutuellement ;
- L'individu s'est plaint qu'il manquait des renseignements précis. L'institution fédérale maintient qu'elle a fourni les dossiers en question, mais accepte de les fournir de nouveau ;

- L'institution fédérale a le droit de refuser accès à certains renseignements, mais l'enquêteur l'a convaincue d'exercer son pouvoir discrétionnaire pour les communiquer ;
- L'enquête a révélé qu'on a traité de façon irrégulière des quantités importantes de renseignements pour un demandeur, et l'institution fédérale accepte de communiquer plus de renseignements pour que la communication soit uniforme.

Dans tous les cas, le Commissariat à la protection de la vie privée a négocié une solution qui satisfait toutes les parties. Il a mené une enquête exhaustive et approfondie et présenté une conclusion officielle aux plaignants. Si le Commissaire conclut que la plainte est résolue, le plaignant a encore le droit d'interjeter appel auprès de la Cour fédérale.

Plainte réglée en cours d'enquête
Cette catégorie constitue non pas un règlement officiel, mais plutôt un moyen acceptable de retirer une plainte lorsque l'enquête est terminée et que le plaignant reconnaît que les efforts du Commissariat à la protection de la vie privée sont satisfaisants et ne veut pas aller plus loin. Par exemple, l'enquêteur explique que les renseignements que le plaignant croyait pouvoir trouver dans les dossiers de l'institution fédérale demeurent introuvables, soit parce qu'ils ont déjà été détruits conformément aux normes établies en matière de conservation et de retrait, ou qu'ils n'ont jamais existé. Toutefois, lorsqu'une plainte est réglée en cours d'enquête, le plaignant peut, par la suite, demander une conclusion officielle. En pareil cas, le Commissaire rouvre le dossier pour que l'enquêteur puisse lui soumettre un rapport officiel, puis le Commissaire explique sa conclusion dans une lettre au plaignant.

Plainte abandonnée
Cette catégorie s'applique aux enquêtes annulées avant que toutes les allégations aient été étudiées. Une plainte peut être abandonnée pour diverses raisons, par exemple, lorsque le plaignant ne veut plus obtenir gain de cause ou que le Commissariat ne peut le retrouver pour en obtenir les renseignements supplémentaires qui permettraient d'arriver à une conclusion. Par exemple, le plaignant peut déménager sans nous laisser d'adresse ou de numéro de téléphone. En pareil cas, la plainte ne débouche sur aucune conclusion officielle.

L'art de lire à l'envers

Une femme a dénoncé son ex-mari et celui-ci l'a su. Y a-t-il eu divulgation abusive ? Pour bien des raisons, l'affaire a été difficile à trancher.

La femme a porté plainte au Commissaire à la protection de la vie privée, accusant le ministère du Développement des ressources humaines Canada d'avoir délibérément et abusivement révélé des renseignements à son sujet. Plus précisément, elle affirmait qu'un enquêteur de DRHC avait révélé à son ex-mari qu'elle avait confié au ministère des renseignements à son sujet. Quelque temps auparavant, elle avait communiqué avec DRHC pour signaler qu'elle soupçonnait son ex-mari d'avoir frauduleusement réclamé des prestations d'assurance emploi.

DRHC a comme politique de protéger l'identité des dénonciateurs. En fait, ces derniers peuvent même réclamer l'anonymat. Dans ce cas-ci toutefois, la femme avait insisté pour laisser son nom et son numéro de téléphone au cas où DRHC aurait besoin de la contacter à nouveau.

Après avoir reçu la déclaration de cette femme, un enquêteur de DRHC a convoqué l'ex-mari à une entrevue, à laquelle celui-ci s'est présenté en compagnie de sa nouvelle épouse. La piste s'est révélée bonne et l'enquête a eu pour résultat l'annulation totale et rétroactive des prestations d'assurance emploi de l'ex-mari.

C'est là que l'histoire prend tout un virage. Après avoir subi une baisse de revenus, l'ex-mari a demandé que ses versements obligatoires de pension alimentaire soient réduits. Par la suite, l'homme a affirmé devant la cour provinciale que, pendant son entrevue avec l'enquêteur de DRHC, sa nouvelle épouse et lui avaient tous deux vu un document indiquant que son ex-femme avait fait une déclaration contre lui.

Après avoir entendu les témoignages, le juge lui a accordé une réduction substantielle de ses paiements de pension alimentaire. L'ex-femme s'est ainsi vue privée d'une bonne partie de l'aide financière dont elle avait grandement besoin pour son enfant. Et même si le juge a nié que le rôle de dénonciatrice de l'ex-épouse ait influencé la décision de la cour, elle n'en était pas plus convaincue.

Vu que la plaignante dépendait dans une certaine mesure des versements de son ex-époux, pourquoi avait-elle tout de même dénoncé celui-ci ? Comme cela arrive souvent dans notre travail, notre enquêteur s'est posé une foule de

questions complexes sur la vie, les rapports et les motifs des diverses parties. Mais, pour le personnel du Commissariat, seule comptait vraiment la question suivante : était-il vrai que des renseignements personnels et confidentiels sur la plaignante avaient été divulgués à l'ex-mari et à sa nouvelle épouse au cours de l'entrevue avec le représentant de DRHC ?

Voici certaines circonstances dont notre enquêteur a dû tenir compte :

- De par son expérience, l'enquêteur de DRHC reconnaissait la valeur des sources d'information et la nécessité de protéger les dénonciateurs. Dans ce cas-ci, il savait à l'avance que l'homme et sa nouvelle épouse soupçonneraient fortement l'ex-épouse d'être l'informatrice (c'est d'ailleurs ce qu'ils lui ont dit pendant l'entrevue). Il savait aussi qu'ils tenteraient probablement de lui soutirer quelque confirmation de leurs soupçons. En homme averti, il s'est présenté dans la salle d'entrevue encore plus déterminé que d'habitude à ne révéler d'aucune façon l'identité de sa source d'information.
- Malgré tout, l'enquêteur de DRHC a emporté son dossier avec lui dans la salle d'entrevue pour s'y référer, comme de coutume. Le dossier contenait entre autres les deux formulaires sur lesquels les renseignements fournis par l'ex-femme avaient été inscrits. Au bas des deux formulaires, le nom et le numéro de téléphone de l'ex-épouse étaient clairement visibles.
- L'enquêteur de DRHC croyait avoir pris toutes les précautions nécessaires lorsqu'il a consulté son dossier pendant l'entrevue. La pièce était petite et ses occupants y étaient relativement à l'étroit, mais il n'avait pas laissé son dossier ouvert et l'avait gardé sous surveillance, et il avait fait bien attention pour que le couple ne puisse lire l'identité de l'informatrice sur les formulaires. Il ne pouvait le nier catégoriquement, mais il doutait fort que le couple ait pu entrevoir des renseignements confidentiels.
- Néanmoins, l'ex-mari a indiqué à notre enquêteur que sa femme et lui avaient justement réussi. Il a dit avoir vu le numéro de téléphone de son ex-épouse et peut-être aussi son nom au bas d'un des formulaires que contenait le dossier de l'enquêteur. Sa nouvelle épouse avait également pu discerner des détails sur le formulaire et, ensemble, ils avaient été en mesure de confirmer l'identité de la dénonciatrice.
- Grâce à une demande en vertu de la *Loi sur la protection des renseignements personnels*, l'ex-mari a obtenu l'accès à son dossier de DRHC, qui contenait les deux formulaires en question. Au bas de ces formulaires,

pour des raisons de confidentialité, le nom et le numéro de téléphone de l'informatrice avaient été dissimulés.

En se basant en grande partie sur la description convaincante qu'avait fait l'ex-mari des sections rayées des formulaires, notre enquêteur était porté à croire qu'il y avait bel et bien eu divulgation pendant l'entrevue. Mais il voulait en être certain. Après tout, quelle était la probabilité que l'ex-mari ait pu lire un des formulaires à l'envers ? L'enquêteur a entrepris de recréer la scène.

Pour simuler la situation d'entrevue, il a placé le formulaire sur un bureau à cinq pieds de lui. Même en regardant le formulaire à l'envers à cette distance, il a constaté qu'il pouvait lire très facilement le numéro de téléphone de la dénonciatrice. Sans trop d'effort supplémentaire, il pouvait également distinguer son nom.

Ce test a suffi à le convaincre. Il a recommandé au Commissaire de déclarer que la plainte de l'ex-épouse était fondée. C'est ce que le Commissaire a fait, mais en ajoutant une importante réserve. Il y avait eu divulgation abusive de renseignements confidentiels, certes, mais celle-ci n'était de toute évidence nullement intentionnelle. Le Commissaire a précisé que l'enquêteur de DRHC avait commis une erreur par inadvertance.

Un consentement bien peu éclairé

Dans le cadre d'un cas bien médiatisé, le plaignant s'est plaint que Revenu Canada avait contrevenu à la *Loi sur la protection des renseignements personnels* en communiquant des renseignements de ses déclarations de revenus à la Manitoba Public Insurance Corporation (MPIC).

Le Commissaire à la protection de la vie privée a conclu que la plainte était fondée. Mais, élément plus important encore, il a proposé des correctifs visant à éliminer un tel manquement à la vie privée, devenu pratique courante au Manitoba.

Le plaignant avait été impliqué dans un grave accident de voiture. Il a par la suite rempli une réclamation de la MPIC, signant par la même occasion un formulaire de consentement qui autorisait la MPIC à enquêter et à consulter le dossier médical et d'employé du plaignant.

La MPIC avait en effet besoin de confirmer le revenu du plaignant, ce qui aurait dû se faire en posant la question à l'employeur. Dans ce cas-ci, comme

souvent d'ailleurs, la MPIC a remarqué une différence, et décidé que la meilleure façon de savoir qui disait vrai était de consulter les déclarations de revenu du plaignant. La MPIC a donc contacté Revenu Canada.

Pas si vite, pourraient dire certains : en effet, ces déclarations de revenu sont soi-disant confidentielles. Revenu Canada a son propre formulaire de consentement que le plaignant n'avait ni vu ni signé. Ce formulaire doit être diligemment signé par le contribuable visé et répondre à une demande claire et sans équivoque avant que le ministère ne communique quelque renseignement que ce soit à une tierce partie. Mais pour la MPIC, rien de tout cela n'a été nécessaire.

Un de ses employés a tout simplement annexé le formulaire de consentement général de la MPIC (signé par le plaignant) au formulaire d'autorisation de Revenu Canada (jamais vu ni signé par le plaignant). Ensuite, l'employé de la MPIC a écrit sur le formulaire vierge de Revenu Canada «Voir autorisation ci-jointe », sans même se donner la peine de préciser les renseignements spécifiquement nécessaires à l'enquête de la MPIC. Une telle « autorisation » semblait donc donner carte blanche à Revenu Canada pour la divulgation non seulement du revenu actuel du demandeur mais bien de tous les autres renseignements contenus dans ses déclarations de revenus des cinq dernières années.

Et c'est ce que la MPIC a obtenu — l'ensemble des déclarations du plaignant pour les cinq dernières années. Demandez et vous recevrez…

Comme notre enquête l'a souligné, c'est de cette façon que la MPIC et Revenu Canada ont *toujours* procédé. La MPIC envoyait plusieurs demandes par semaine au bureau local de Revenu Canada, auxquelles le personnel de ce dernier répondait de façon routinière sans jamais vérifier si le formulaire de consentement général de la MPIC constituait une autorisation suffisante pour la communication de renseignements fiscaux. Et Revenu Canada faisait plus souvent qu'autrement preuve d'une grande générosité en communiquant à la MPIC beaucoup plus de renseignements que nécessaire.

La MPIC n'avait jamais remis en question son droit à de tels renseignements. En effet, ses employés croyaient que leur formulaire de consentement général leur conférait accès à l'ensemble des déclarations de revenus d'un contribuable, même si seul un renseignement leur suffisait.

Le Commissaire à la protection de la vie privée n'était pas d'accord. Au contraire, il ne pouvait que conclure au fait que Revenu Canada avait profondément porté atteinte aux droits du plaignant en vertu de la *Loi sur la*

protection des renseignements personnels en divulguant ses déclarations de revenus sans son consentement. Le mal étant fait, cependant, le Commissaire a néanmoins pris les mesures nécessaires afin qu'aucun autre contribuable n'ait à subir une pareille atteinte à ses droits à l'avenir.

Il s'est tout d'abord assuré que les déclarations de revenus du plaignant quittent les locaux de la MPIC. Puis il a rappelé pour le bénéfice de tous la nécessité d'un formulaire de consentement clair, précis et signé pour autoriser la communication de renseignements fiscaux. Enfin il a recommandé que Revenu Canada cesse sa pratique de communiquer des renseignements à la MPIC tant qu'une entente précise à ce chapitre ne serait pas intervenue entre les deux organismes.

Revenu Canada a cessé ses communications à la MPIC à compter du 27 avril 1999. Le Commissaire à la protection de la vie privée effectuera un suivi afin de s'assurer que l'éventuelle entente entre les deux organismes est appropriée et conforme à la *Loi sur la protection des renseignements personnels.*

Entre-temps, si la MPIC a besoin de vérifier le revenu d'un demandeur, ce sera à ce dernier d'obtenir ses propres renseignements de Revenu Canada.

Vous pourriez être quelqu'un d'autre !

Trois amis entrent dans un magasin. Deux en ressortent avec des achats. Le troisième quant à lui repart les mains vides et humilié d'avoir été pris pour un criminel.

Au départ ces personnes comptaient se procurer des armes à feu en conformité avec les strictes procédures d'enregistrement maintenant en vigueur. Les trois ont fidèlement rempli les demandes à cette fin et l'employé a procédé à une interrogation électronique d'une base de données appelée « PIAF » — Personnes d'intérêt relatif aux armes à feu. Deux des demandes ont été vérifiées sans problème, mais la troisième a essuyé un refus automatique. La raison donnée par l'ordinateur était laconique : « Nouvelles informations concernant le demandeur ».

Une fois refusée, la demande a été acheminée électroniquement au Contrôleur des armes à feu pour l'Ontario. Moins de 24 heures plus tard, le refus initial était renversé et la demande approuvée.

Mais plusieurs questions demeuraient sans réponse. Pourquoi le refus initial ? Pourquoi une demande antérieure par le même acheteur avait-elle été

approuvée sans problème un mois avant ? À quelles sortes de nouvelles informations, la vérification informatique faisait-elle référence ?

Le demandeur a demandé au ministère de la Justice de s'expliquer. On lui a dit que la recherche menée avait confondu son nom avec celui d'une personne possédant la même date de naissance et connue des forces policières. Le demandeur s'est alors satisfait de cette explication, du moins jusqu'à ce qu'un incident similaire se reproduise.

Le deuxième refus s'est produit un mois plus tard lorsque la demande d'arme à feu a été rejetée pour le même motif. Une fois de plus, le demandeur a été profondément humilié par les regards soupçonneux des employés et des clients du magasin. Une fois de plus, l'erreur était découverte par le Contrôleur en moins de deux jours, le refus initial rejeté et l'achat de l'arme autorisé. La base de données PIAF avait de nouveau confondu le nom du demandeur avec celui d'une personne n'ayant pas le droit de se procurer des armes à feu.

Cette fois cependant, le demandeur ne s'est pas contenté de la simple explication orale du ministère. Qu'une erreur d'identification se produise une fois, passe encore. Mais pas deux. Et il n'entendait pas revivre le même cauchemar à chaque fois qu'il ferait une demande de permis d'armes à feu comme on le lui avait laissé entendre. Il a décidé de régler la question en soumettant des demandes d'accès à l'information au ministère de la Justice et à la Gendarmerie royale du Canada en vertu de la *Loi sur la protection des renseignements personnels*.

En réponse à sa demande d'une explication écrite détaillée, le ministère de la Justice ne lui a expédié que des copies de ses trois demandes d'arme à feu. Les deux demandes qui avaient été initialement rejetées ne portaient aucune autre explication que la note originale « Nouvelles informations concernant le demandeur ». La lettre de réponse du ministère précisait qu'il n'incombait pas à ce dernier d'expliquer la chose, mais seulement d'identifier et de réviser les dossiers demandés.

Le demandeur a alors déposé une plainte en vertu de la *Loi sur la protection des renseignements personnels* alléguant qu'il n'avait pas reçu d'explications écrites des refus temporaires qu'il avait essuyés en tentant d'acheter des armes à feu.

La base de données PIAF ne fournissait en elle-même aucune explication. Les responsables du ministère de la Justice ont souligné à notre enquêteure que toute interrogation de la base de données est strictement électronique, ne permettant même pas l'impression du contenu affiché à l'écran. Notre

enquête parallèle auprès de la GRC nous a cependant donné accès à d'autres banques de données plus éclairantes.

Notre enquêteure a été éventuellement en mesure d'identifier la personne dont le nom et la date de naissance avaient été pris pour celles du plaignant. En fait, les dates de naissance différaient de cinq mois, et les noms étaient aussi dissemblables que « Savoie » et « Savard ». Ces différences, apparemment, importaient peu à un ordinateur « capable » de reconnaissance de la voix.

Notre enquêteure a quand même réalisé certains progrès pour l'avenir, grâce notamment au solide appui du plaignant qui a de son côté écrit nombre de lettres et fait nombre d'appels téléphoniques.

Nous avons réussi à convaincre les responsables du ministère de la Justice de modifier la base de données PIAF afin de dissocier le plaignant de l'autre individu, du moins dans le contexte actuel. Ils y sont parvenus en effaçant le code séquentiel assigné à la dernière confrontation entre cet individu et les forces policières. Le ministère a cependant précisé que si cet individu — ou n'importe quel autre individu ayant un nom, une date de naissance ou une adresse similaire — avait d'autres démêlés avec la justice, un nouveau code séquentiel serait assigné, ce qui amènerait probablement une autre confusion avec le nom du plaignant. Dans une telle éventualité, ce dernier devrait communiquer avec le ministère afin que son personnel efface le tout dernier code.

Même si nous devons taire le nom de l'autre individu, et malgré le risque d'une autre confusion de noms à l'avenir, le plaignant s'estime relativement satisfait des progrès de notre enquête. En effet, ce ne sont pas les ennuis ou les retards qui l'avaient poussé à se plaindre. Bien d'autres innocents intéressés à acheter une arme à feu — dont tous les Tremblay et les Smith du pays — ont certainement dû passer par des ennuis et des retards autrement plus graves que les siens. Le plaignant ne s'oppose pas non plus à l'existence de la base de données PIAF ni à l'enregistrement des armes à feu.

Tout ce qu'il souhaitait en fait était une explication écrite de ce qui s'était passé, qu'il pourrait porter sur lui afin de prouver aux amis, commis et clients qu'il n'était pas un criminel.

Une fois l'assurance obtenue qu'une telle explication serait inclue dans le rapport que nous lui ferions parvenir, il a accepté que sa plainte contre le ministère de la Justice soit « résolue en cours d'enquête ».

Rappelons que le Commissariat est en train d'étudier toute la question de la gestion des renseignements personnels dans le cadre du programme d'enregistrement des armes à feu.

Abus de pouvoir

Il n'est pas inhabituel qu'un candidat ayant échoué à un concours pour un emploi au sein du gouvernement fédéral interjette appel. Il est cependant inhabituel qu'un témoin de ce candidat subisse l'humiliation de voir ses renseignements personnels jetés sur la place publique. Inhabituel, mais possible, comme le prouve le cas suivant.

Le Commissaire à la protection de la vie privée ne veut pas qu'un tel cas se reproduise.

Une employée fédérale échoue à un concours interne d'embauche. Lorsqu'elle entreprend des démarches pour interjeter appel devant le Comité d'appel de la Commission de la fonction publique, le syndicat demande à un collègue de travail de témoigner en son nom.

Sa direction s'oppose immédiatement au témoignage du collègue. Dans une présentation officielle au Comité d'appel, la direction s'explique et conclut en avertissant que si ce collègue et un certain autre sont appelés à témoigner, l'institution fédérale tentera de discréditer non seulement les témoignages, mais également la « crédibilité des témoins ».

Ironiquement, le collègue cité n'avait jamais souhaité être témoin. En fait, il avait d'abord décliné la demande. Il ne semblait pas non plus être particulièrement bien disposé à l'égard de la candidate interjetant appel. Néanmoins, le syndicat croyait qu'il détenait de l'information sur le concours pouvant peut-être appuyer la cause. Le Comité d'appel l'a donc cité à comparaître, et il a accepté.

Durant l'appel, la direction a donné suite à sa menace. Durant le contre-interrogatoire, le représentant de la direction s'est obstinément attaqué non seulement au témoignage, mais aussi à la crédibilité du collègue de travail. Et les questions ont de plus en plus dévié vers des domaines dont l'intérêt était mis en doute par le président du Comité d'appel.

Finalement, les questions ont porté sur un point délicat et tout à fait hors de propos : le récent congé de maladie prolongé pris par le témoin et les raisons médicales qui le justifiaient. Ces questions insidieuses touchaient à des détails

personnels et trahissaient une solide connaissance des antécédents médicaux du témoin. En fait, elles ne pouvaient avoir été conçues que par quelqu'un ayant lu les fiches de présence personnelles et confidentielles du témoin.

Le président a rapidement mis fin à l'interrogatoire, mais le dommage était fait. Le Comité d'appel était maintenant au courant de renseignements délicats et confidentiels, et le témoin avait été humilié publiquement. Quelques semaines plus tard, encore ébranlé par le contre-interrogatoire, le témoin a déposé une plainte auprès du Commissariat à la protection de la vie privée.

Comment le représentant de la direction avait-il pu accéder aux fiches de présence du témoin? L'enquête a révélé que cela lui avait été très facile. Le représentant était également gestionnaire du personnel au sein de l'institution fédérale. Dans l'exercice normal de ses fonctions, il avait couramment accès aux fiches de présence des employés, y compris aux certificats médicaux. De ce fait, il connaissait à l'avance tout sur le congé prolongé du témoin, ses raisons médicales et le traitement suivi. Par conséquent, la personne qui faisait subir le contre-interrogatoire connaissait non seulement les antécédents médicaux du témoin, mais elle participait également à la procédure avec la ferme intention de dévoiler ces antécédents pour le discréditer.

Le représentant de la direction était en droit de connaître les antécédents du témoin à titre de gestionnaire du personnel. Toutefois, en tant que « contre-interrogateur », il n'avait aucunement le droit de divulguer ces renseignements. Les articles 7 et 8 de la *Loi sur la protection des renseignements personnels* interdisent aux institutions fédérales de se servir ou de divulguer des renseignements personnels sans le consentement de l'intéressé, sauf aux fins pour lesquelles ces renseignements ont été recueillis ou qui sont compatibles avec ces fins.

Le Commissaire à la protection de la vie privée a conclu que les renseignements relatifs au congé de maladie, à la nature de celle-ci et au traitement médical subséquent du témoin étaient sans intérêt à l'audience du Comité d'appel. Il a donc déclaré que la plainte était fondée et qu'elle devait être prise au sérieux.

Le Commissaire s'est dit particulièrement préoccupé d'apprendre que ce n'était pas la première fois que ce gestionnaire du personnel divulguait des renseignements de façon abusive. De fait, le Commissaire se rendait de plus en plus compte que le gestionnaire croyait à tort que son poste lui permettait d'utiliser et de divulguer à son gré les renseignements personnels de

n'importe quel employé.

Par conséquent, le Commissaire a recommandé à l'institution fédérale d'expliquer à ce gestionnaire et à tous les autres gestionnaires et employés leurs obligations concernant la divulgation de renseignements personnels aux termes de la *Loi sur la protection des renseignements personnels*. Le Commissaire a l'intention de surveiller de près les efforts de l'institution fédérale à cet égard.

Un justicier controversé

Dans l'ensemble, la Gendarmerie royale du Canada s'en tire remarquablement bien dans le domaine du respect des droits à la vie privée. Cela est en soi assez surprenant compte tenu de la quantité et du type de renseignements personnels que cet organisme recueille et des multiples possibilités d'abus. Mais le Commissaire à la protection de la vie privée évalue la GRC comme étant non seulement l'organisme fédéral le plus respectueux des lois, mais aussi le plus coopératif et rempli de bonne volonté lorsque des correctifs s'imposent.

Malheureusement, il y a toujours certains manquements. Ainsi, il arrive à l'occasion que les initiatives d'un policier trop bien intentionné et zélé dépassent les bornes.

Tel a été le cas l'année dernière, d'un gendarme albertain qui en est venu à la conclusion que la simple application de la loi quant au port de la ceinture de sécurité était insuffisante. Il a donc entrepris de *renforcer* la loi et ce d'une manière bien particulière.

Un conducteur albertain s'est plaint au Commissaire à la protection de la vie privée que la GRC avait indûment communiqué ses renseignements personnels. Plus précisément, il prétendait qu'une copie d'une contravention reçue pour ne pas avoir bouclé sa ceinture de sécurité avait été expédiée à sa compagnie d'assurance par le policier qui l'avait émise.

Malheureusement, l'histoire s'est avérée exacte. Notre enquête a révélé que l'agent en question avait procédé ainsi, et ce à plusieurs reprises. L'agent a lui-même admis avoir effectivement communiqué pendant trois ou quatre mois avec les compagnies d'assurance de 10 à 20 personnes ayant enfreint les dispositions régissant le port de la ceinture de sécurité.

Il a expliqué être à l'origine de ce « projet pilote ». Effectivement, la GRC de l'endroit menait bien une campagne pour encourager le port de la ceinture de

sécurité, mais seul un policier avait eu recours à de pareilles mesures. Celui-ci a expliqué qu'à son avis les contrevenants ne tarderaient pas à boucler leur ceinture de sécurité s'ils subissaient une augmentation de leurs primes d'assurance *en sus* de devoir acquitter les contraventions reçues.

Il n'avait pas réalisé qu'en agissant ainsi à l'endroit d'une catégorie de contrevenants, il transgressait à son tour les droits des citoyens canadiens en vertu de la *Loi sur la protection des renseignements personnels*. L'article 8 de la Loi interdit la communication des renseignements personnels d'une personne sans son consentement, sauf dans les cas d'exceptions énumérés au paragraphe 8(2) de la Loi.

Dans le cas présent, le Commissaire à la protection de la vie privée n'a pu trouver aucune exception pertinente, et en a conclu que la plainte était fondée puisque le gendarme n'avait pas tenu compte des dispositions de la *Loi sur la protection des renseignements personnels* lors du lancement du projet pilote. Le Commissaire a en outre tenu à souligner à la GRC qu'une semblable divulgation portait sérieusement atteinte aux droits individuels conférés par la *Loi sur la protection des renseignements personnels*.

À la décharge de la GRC, ses responsables ont mis fin au projet pilote dès qu'ils en ont été informés. À notre suggestion, ils ont fait le tour de tous les détachements de l'Alberta en vue de s'assurer que personne d'autre n'avait eu d'idée semblable, ce qui n'était pas le cas. Il s'agissait bien d'une opération solo.

En conclusion, l'initiative de l'agent n'a pas reçu beaucoup d'appuis. Mais qu'en ont pensé les compagnies d'assurances ? L'augmentation possible des primes d'assurances a-t-elle influencé leur intérêt ?

Pour certaines compagnies, peut-être. Mais certainement pas pour d'autres : c'est la propre compagnie d'assurance du plaignant qui a initialement porté cette question à l'attention du Commissariat.

Un colis bien dur à retrouver

Le cas a trait à trois plaintes déposées par une même personne contre deux organismes différents, et il n'est toujours pas résolu. Heureusement, l'une de nos enquêteures a pu aller plus ou moins au fond des choses en persuadant la Société canadienne des postes (SCP) d'y regarder d'un peu plus près.

Deux mois après avoir soumis une demande d'accès à ses renseignements en

vertu de *la Loi sur la protection des renseignements personnels*, le plaignant déposait sa première plainte à l'effet que Revenu Canada (RC) tardait à lui répondre. Alors que notre Commissariat se penchait sur cette plainte de délais, RC nous avisait qu'il venait juste de répondre au plaignant en lui faisant parvenir un colis à son adresse postale.

Le Commissariat à la protection de la vie privée a alors classé cette plainte de délais comme fondée mais résolue. Le colis, lui, n'était cependant pas parvenu à destination.

On s'est alors aperçu qu'il avait bien été envoyé à la bonne personne, mais au mauvais casier postal — une erreur d'un seul chiffre. RC et la SCP ont alors tenté de retracer l'envoi, mais n'ont pu retrouver qu'un simple récépissé établissant que le colis avait bien été livré à la bonne succursale postale, mais qu'une personne autre que le destinataire en avait accusé réception.

Une seconde plainte a alors été déposée contre la SCP en vertu de la *Loi sur la protection des renseignements personnels* à l'effet que l'organisme aurait communiqué les renseignements personnels du plaignant en permettant à une tierce personne lors de la livraison d'accuser réception du colis. De plus, malgré le récépissé, le colis manquait toujours à l'appel.

Le plaignant lui-même s'est informé auprès de la succursale postale, où des employés lui ont confirmé avoir fouillé sans succès les lieux. D'après eux, où que soit le colis, il n'était pas chez eux.

En dépit de tout cela, notre enquêteure a avisé la SCP qu'elle comptait visiter la succursale postale en question. Elle obtenait aussi qu'une nouvelle fouille des lieux soit entreprise et que l'on y garde le colis sur place jusqu'à son arrivée si jamais celui-ci refaisait surface. Avant même de partir, le siège social de la SCP l'avisait du succès de l'opération à la succursale postale.

À son arrivée sur les lieux, des représentants de la SCP attendaient notre enquêteure pour lui communiquer la bonne nouvelle. La fouille demandée avait permis de retrouver le colis par terre, enfoui sous plusieurs colis de Noël et d'autre courrier.

La SCP s'est perdue en conjonctures quant à savoir comment le colis s'était retrouvé là. Une possibilité est que le facteur en ait effectué la livraison à la succursale postale qui aurait alors oublié le colis de côté puisque l'adresse ne correspondait pas à aucune des cases postales existantes.

Mais alors comment expliquer le récépissé et la signature provenant d'une

autre personne que le destinataire ? La SCP croit possible que le facteur ait en fait accidentellement livré le colis à une tierce personne qui en aurait accusé réception. Ayant alors constaté son erreur, cette tierce personne aurait rapporté le colis à la succursale postale figurant à l'adresse. Une fois là, aux prises avec un colis adressé à une case postale inexistante, les employés l'aurait simplement mis de coté et oublié.

Cette théorie achoppe sur le fait qu'aucun employé ne se souvient d'une telle livraison. Un autre obstacle tient au fait que la personne présumée avoir accusé réception du colis (selon les noms des clients de la succursale) nie avoir reçu ou accepté un colis adressé au plaignant. De fait, les initiales et la signature de cette personne ne correspondent pas à celles du client de la succursale partageant son nom de famille.

Il est possible que le mystère ne soit jamais éclairci mais au moins, le plaignant a été satisfait puisque notre enquêteure lui a remis son colis en mains propres. Frustré à juste raison par les délais, le récipiendaire s'est déclaré satisfait de recevoir le colis cacheté et intact. Il a accepté de considérer la seconde plainte comme résolue.

Et sa troisième plainte ? Celle-ci a été déposée un peu plus tard après que le plaignant a pris connaissance du contenu de l'envoi et questionne certaines exemptions appliquées aux renseignements recherchés. Au moment d'aller sous presse, la troisième plainte n'était pas encore résolue.

Entre-temps, en ce qui a trait aux colis mal adressés, la SCP affirme que la politique officielle *n'est pas* de mettre ceux-ci de coté et de les reléguer aux oubliettes.

Mais qui est responsable, au juste ?

Pour la première — et peut-être la dernière — fois, le Commissariat fédéral à la protection de la vie privée s'est penché sur une plainte ayant trait aux dossiers d'un jeune contrevenant. En fait, l'enquête menée a permis d'établir que de tels dossiers se situaient bien au-delà de la *Loi sur la protection des renseignements personnels*.

Une plainte a été déposée en vertu de cette dernière Loi contre le ministère de la Justice. Le plaignant soutenait s'être vu refuser accès au mémoire de la Couronne concernant une poursuite au criminel en vertu de la *Loi sur les jeunes contrevenants*. Le plaignant prétendait que le jeune en question était son client (point sur lequel nous reviendrons plus tard).

Comme notre enquêteure a pu le découvrir, le refus d'accès du ministère découlait de l'absence des renseignements demandés. Quoique la *Loi sur les jeunes contrevenants* soit fédérale, son administration relève du provincial. Les renseignements recherchés par le demandeur n'étaient pas détenus par le gouvernement fédéral mais plutôt par le gouvernement provincial concerné, soit l'Ontario.

Une fois prévenu, le plaignant a demandé au gouvernement ontarien de lui remettre les renseignements en vertu de la loi provinciale d'accès à l'information. Mais le Solliciteur général de l'Ontario l'a informé plutôt maladroitement que les renseignements voulus ne relevaient pas de la loi provinciale, mais bien de la fédérale qui avait préséance.

À quelle loi fédérale le vérificateur général faisait-il référence ? À la *Loi sur les jeunes contrevenants*. Et le plaignant ? À la *Loi sur la protection des renseignements personnels*. Pourquoi le Solliciteur général n'a-t-il pas fait preuve de plus de précision ? Simplement parce qu'en précisant qu'il s'agissait bien de la *Loi sur les jeunes contrevenants*, on aurait identifié le jeune comme contrevenant, ce qui est expressément interdit par cette dernière Loi.

Le plaignant a donc entamé à tort des procédures en vertu de la *Loi sur la protection des renseignements personnels*. Mais le Commissaire à la protection de la vie privée a été dans l'impossibilité de lui venir en aide. Éventuellement, notre enquêteure et plusieurs représentants tant du provincial que du fédéral en sont venus à la conclusion que la *Loi sur la protection des renseignements personnels* n'a pas préséance sur la *Loi sur les jeunes contrevenants*, laquelle possède ses propres dispositions quant à la communication de renseignements. Plus précisément, l'article 44(1) de la Loi autorise la communication des renseignements concernant un jeune contrevenant, mais plus aux parents ou représentants une fois la poursuite au criminel terminée. Par ailleurs, puisque ce sont les provinces qui administrent la *Loi sur les jeunes contrevenants*, ce sont les procureurs provinciaux de la Couronne qui déterminent les renseignements susceptibles d'être communiqués en vertu de la Loi.

En ce qui concerne la question des représentants, il y a un coté intéressant à ce cas. Notre enquêteure a en effet découvert que le plaignant avait déjà suivi cette avenue. Il avait déposé une demande en vertu de l'article 44(1) de la *Loi sur les jeunes contrevenants* mais la Couronne au local lui avait refusé accès en alléguant qu'il n'était pas un adulte apte à représenter le jeune.

Dès le début, notre enquêteure avait conçu des soupçons quant à la légitimité du statut du représentant du jeune contrevenant. Si les choses s'étaient

déroulées autrement, elle aurait pris les mesures nécessaires pour en vérifier l'authenticité.

En bout de ligne, la question de la représentation était sans intérêt pour le Commissaire à la protection de la vie privée. Puisque l'accès aux renseignements des jeunes contrevenants est délimité par la *Loi sur les jeunes contrevenants* et parce qu'une telle information n'est pas conservée par le gouvernement fédéral, le Commissaire a été dans l'impossibilité de conclure au non-respect de *la Loi sur la protection des renseignements personnels*. La plainte a été jugée non fondée.

Des conducteurs manitobains jetés aux ordures

En janvier 1999, le personnel d'Élections Canada a perdu une bande informatique.

Une perte plutôt embarrassante, par ailleurs, car cette bande informatique ne contenait rien de moins que plein de renseignements personnels sur la majorité des Manitobains d'âge adulte. Fait encore plus troublant, cette bande n'a jamais été retrouvée.

Y figuraient plus précisément les noms, adresses, dates de naissance et numéros de permis de conduire de quelque 675,000 conducteurs manitobains. La direction provinciale des véhicules avait envoyé cette bande par messagerie à Élections Canada, dont le personnel s'en serait servi pour la mise à jour des listes électorales.

La *Loi électorale du Canada* autorise Élections Canada a conclure des accords d'échange de renseignements avec divers organismes fédéraux, provinciaux et territoriaux aux fins de la mise à jour du Registre national des électeurs. À l'heure actuelle, Élections Canada reçoit quatre fois par année des renseignements confidentiels en provenance de 27 sources. Dans le cas présent, le recours à une bande informatique était prévu dans l'entente entre le Manitoba et le Directeur général des élections du Canada.

La perte des renseignements personnels était quant à elle tout à fait imprévue. Toutes les ententes, dont celle avec le Manitoba, prévoient qu'Élections Canada prendra toutes les mesures de protection et de sécurité nécessaires au maintien de la confidentialité des renseignements personnels qui lui sont confiés. Suite à cet incident, le ministère manitobain de l'infrastructure et des transports a suspendu l'application de l'entente tant que le mystère ne serait pas résolu et que des correctifs satisfaisants ne seraient

pas mis en place.

De son coté, Élections Canada ne pouvait pas se permettre de prendre la question à la légère. En effet, comme le bon fonctionnement de cet organisme dépend en grande partie des renseignements lui provenant de l'extérieur, son personnel et sa gestion ne savaient que trop les graves conséquences que pourrait avoir un tel incident sur d'autres protocoles d'échange de renseignements. D'entrée de jeu, Élections a donc tout mis en œuvre pour rassurer ses fournisseurs et le public sur ses aptitudes à gérer et protéger les renseignements personnels qui lui sont confiés.

Après avoir en vain fouillé ses locaux de fond en comble à cinq reprises, Élections Canada a averti les représentants manitobains de la perte encourue, puis a immédiatement exigé une vérification indépendante de ses procédures internes de sécurité et de gestion des données. Plusieurs des recommandations découlant de cette vérification ont depuis été mises en œuvre, améliorant ainsi encore davantage les composantes humaines et techniques d'un système déjà hautement sophistiqué, mais visiblement imparfait.

Élections Canada a cependant omis d'avertir le Commissaire fédéral à la protection de la vie privée, lequel n'a eu vent de l'incident que plus de deux mois plus tard, suite à un appel de l'Ombudsman du Manitoba.

Malgré la vérification indépendante déjà effectuée pour le compte d'Élections Canada, le Commissaire a donc décidé de mener sa propre enquête, multipliant les visites de sites et de longues entrevues avec tous les fonctionnaires impliqués. Le personnel du Commissariat n'a pu que corroborer les conclusions tant d'Élections Canada que celles provenant de la vérification indépendante.

- La bande manquante avait bel et bien été reçue aux bureaux d'Élections Canada et récupérée à la salle de courrier tel qu'attesté par son personnel, y compris l'employé qui l'avait prise.
- Faute de preuves, l'enquête a révélé qu'il était improbable qu'un employé ou un inconnu ait volé la bande. Tous les employés rencontrés se sont montrés francs, coopératifs et crédibles. En outre, le haut degré de sophistication du système de sécurité en place rend improbable la possibilité qu'un intrus ait pu s'emparer de la bande et s'enfuir sans être détecté.
- La bande a probablement été accidentellement mise à la poubelle. Ainsi, le jour même de l'incident, l'employé qui s'était rendu à la salle de

courrier était préoccupé par la santé de sa nouvelle petite fille et avait hâte de rentrer à la maison avec la permission de ses patrons. Revenu à son bureau, il aurait mis la nouvelle enveloppe contenant la bande par-dessus cinq autres enveloppes de messagerie déjà vides et à jeter. Pressé et distrait, l'employé pourrait très bien avoir mis la nouvelle enveloppe, encore cachetée, à la poubelle en même temps que les cinq vieilles.

- C'est au cours d'une vérification de routine menée trois jours plus tard que l'employé a remarqué l'absence de la bande informatique du Manitoba. Mais les poubelles de cette journée-là avaient déjà été vidées depuis un bon moment et leur vieux contenu était à des kilomètres. (En raison de leur enduit ciré, les enveloppes de messagerie ne sont pas recyclées, mais jetées dans un site d'enfouissement avec le reste des ordures non recyclables.)
- Quoi qu'il soit advenu de la bande informatique, il est peu probable qu'une personne non autorisée ait pu accéder aux renseignements confidentiels qu'elle contenait. Rien n'identifiait la nature, la source ou le destinataire de la bande, et les renseignements étaient codés d'une façon unique aux gros ordinateurs IBM et illisibles sans logiciel spécial.

Le Commissaire à la protection de la vie privée a conclu qu'une erreur humaine était à l'origine de la perte de la bande magnétique, que le rapport de la vérification extérieure était complet et crédible, et qu'il était satisfait des correctifs mis de l'avant par Élections Canada pour éviter qu'un pareil incident ne se reproduise.

Le Commissaire a indiqué à l'Ombudsman du Manitoba et au Directeur général des élections du Canada qu'il était convaincu que la bande informatique avait bel et bien abouti dans un sac à poubelle enterré au site d'enfouissement.

Avec un peu de chance, elle y restera.

Une négligence qui aurait pu être dangereuse

Lorsque certains détenus d'un établissement fédéral ont obtenu accès à des renseignements confidentiels sur tous leurs codétenus, les conséquences ont heureusement été moins graves qu'elles auraient pu l'être. Depuis, le Service correctionnel du Canada (SCC) s'est fait un point d'honneur de compter moins sur la chance à l'avenir.

Une des premières mesures adoptées par le SCC a été de porter l'incident à

l'attention du Commissaire à la protection de la vie privée. Toutes nos enquêtes ne découlent pas de plaintes formulées par de simples citoyens. Il arrive parfois, comme dans ce cas-ci, que les ministères fédéraux rapportent eux-mêmes les incidents justifiant l'attention du Commissaire.

Dan ce cas-ci, le SCC a rapporté que des agents du pénitencier de Kingston avaient trouvé, sur le disque dur d'un ordinateur placé dans la cellule d'un détenu, deux chiffriers contenant de l'information sur plus de 300 détenus du pénitencier. Ces renseignements comprenaient non seulement les noms et des dates repères mais le détail des crimes et des sentences, des numéros confidentiels de casiers judiciaires, ainsi que des annotations concernant les problèmes de santé mentale, le comportement en prison et le risque d'évasion de chaque détenu.

Cet incident a rapidement été signalé à la presse, qui a reçu une copie illicite des chiffriers en cause. Des journalistes se sont inquiétés des dangers que pouvait poser la divulgation de tels renseignements pour les détenus, notamment ceux identifiés comme agresseurs sexuels.

Le jour de l'incident, le personnel du pénitencier a retiré l'ordinateur et l'ensemble des disquettes de la cellule du détenu en cause. Celui-ci a admis avoir reçu ces fichiers sur disquette d'un autre détenu plusieurs mois plus tôt et les avoir copiés sur son disque dur. Il a aussi indiqué savoir que d'autres détenus possédaient les mêmes fichiers.

La journée suivante, le personnel a mené une « fouille exceptionnelle » de l'institution, saisissant tous les ordinateurs et disquettes en possession des détenus ou qui leur étaient autrement accessibles. Cette fouille n'a mis à jour qu'une autre copie des fichiers en question.

La prochaine étape a consisté à communiquer avec toutes les personnes dont la confidentialité avait été compromise. Après avoir remis au Commissariat une copie du modèle de cette lettre, le SCC a envoyé des lettres d'avis appropriées aux 333 détenus concernés, les informant, entre autres, de leur droit de porter plainte en vertu de la *Loi sur la protection des renseignements personnels*. Pour le Commissariat, le fait de prévenir les détenus indiquait clairement que le SCC assumait la responsabilité de l'incident et qu'il était prêt à remédier à une situation grave.

Promettant de tenir le Commissariat informé de l'ensemble des développements, le bureau régional de l'Ontario du SCC a alors amorcé sa propre enquête sur l'incident, qui a mis en lumière les faits suivants :

- Les chiffriers avaient d'abord été créés par un agent du pénitencier.
- Depuis, plus d'un membre du personnel avait participé à la mise à jour de l'information contenue dans les fichiers.
- On savait que les fichiers avaient été stockés dans deux ordinateurs utilisés par le personnel : 1) un ordinateur portatif, que plusieurs membres du personnel avaient souvent amené chez eux, et 2) un ordinateur de bureau, qui avait par la suite été prêté pour utilisation par les détenus. L'un ou l'autre de ces appareils, ou les deux, avaient pu être la source de la communication non autorisée de renseignements personnels.
- L'ordinateur portatif avait disparu un an plus tôt. Aucun système de surveillance ou de suivi de son utilisation n'était alors en place. Donc, aucune piste de documents n'avait été disponible pour contribuer à sa localisation.
- Lorsque l'ordinateur portatif avait disparu, le SCC avait négligé d'avertir le Commissaire à la protection de la vie privée des renseignements personnels contenus sur le disque dur de l'appareil.
- Il était possible qu'avant d'être prêté à un détenu, l'ordinateur de bureau n'avait pas été « nettoyé » (c.-à-d. qu'on n'avait pas effacé de son disque dur les fichiers non appropriés). Même si le service de l'informatique se livrait habituellement à des procédures de nettoyage, leur vérification était informelle et peu rigoureuse. Dans ce cas particulier, aucun document ne permettait de vérifier que l'ordinateur avait bel et bien été nettoyé.

Le rapport d'enquête du SCC en venait à la conclusion que c'est un défaut de procédure, et non les détenus, qu'il fallait blâmer pour cette communication non autorisée de renseignements personnels. Le rapport comprenait trois recommandations musclées touchant des procédures plus serrées de contrôle des prêts d'équipement, le nettoyage d'ordinateurs et le stockage et la sécurité des données.

Le Commissariat est satisfait de l'enquête du SCC et croit que, si elles sont bien appliquées, les mesures recommandées réduiront le risque de nouveaux incidents. De plus, le Commissariat considère les mesures adoptées en réaction à l'incident comme des indications positives de l'engagement continu du SCC à l'égard des principes de la *Loi sur la protection des renseignements personnels.*

Protégeons nos renseignements à l'extérieur du bureau

Les employés fédéraux qui emportent du travail hors du bureau ne bénéficient d'aucune immunité spéciale contre le vol. En fait, comme l'ordinateur portatif est devenu aujourd'hui l'outil idéal pour transporter des dossiers, le personnel doit être particulièrement sur ses gardes. Les dimensions restreintes et la valeur marchande élevée des portatifs en font des cibles très tentantes pour les voleurs.

L'an dernier, lorsque quelqu'un a volé une petite mallette dans la voiture d'un employé, la Société de crédit agricole (SCA) a bien réagi en avertissant le Commissaire à la protection de la vie privée. Cette mallette, qui avait été placée dans le coffre fermé à clef, contenait un ordinateur portatif et un imprimé de renseignements sur les prêts personnels consentis à certains clients de la SCA.

La SCA a mené une recherche approfondie du secteur. L'ordinateur a bientôt été retrouvé, non endommagé, à côté d'un conteneur à déchets, près de l'endroit où la voiture de l'employé était garée. Mais le dossier imprimé n'a pas été localisé.

La SCA a écrit aux clients concernés, les avertissant de la perte de ces renseignements personnels. Depuis, les clients ont reconnu cette perte, sans paraître s'en être offusqués de façon permanente. Du moins, ils ont accepté de continuer à traiter avec la SCA.

La SCA a aussi adressé une note de service à tout son personnel pour lui rappeler l'importance de mettre en sûreté les renseignements personnels. Cette note de service rappelait notamment que :

- les dossiers de clients qui doivent être transportés doivent être gardés dans un attaché-case verrouillé et conservé en possession de l'employé(e) ;
- de tels dossiers doivent être retournés au bureau aussitôt que possible ;
- dans les situations où il est inévitable d'amener des dossiers chez soi, ceux-ci doivent être entreposés dans un endroit sécuritaire, de préférence dans un classeur verrouillé ;
- tout ordinateur portatif apporté à la maison doit demeurer avec l'employé en tout temps et ne doit pas être entreposé dans un véhicule ou dans des bagages.

Dans ce cas-ci, les agents de la SCA n'ont pu établir si des renseignements personnels avaient été stockés dans l'ordinateur. De toute façon, ils doutaient que les voleurs aient eu le temps ou la capacité d'avoir accès à l'information inscrite sur le disque dur, notamment parce que le système d'exploitation de l'appareil était protégé par un mot de passe. Vu les circonstances de la récupération de l'ordinateur, les agents ont jugé que les voleurs avaient dû être interrompus en cours de délit.

Tout en donnant un aval général aux efforts entrepris par la SCA en réaction à la communication non autorisée de renseignements personnels, le Commissaire à la protection de la vie privée a ressenti la nécessité d'émettre un commentaire au sujet de la sécurité des renseignements personnels inscrits dans les ordinateurs portatifs. Il a fait valoir que, même si un ordinateur peut être volé pour la valeur de l'appareil lui-même, il y a toujours une possibilité que l'information stockée dans l'ordinateur soit utilisée au détriment des personnes concernées par cette information.

Quant au fait que la SCA compte sur un simple mot de passe pour interdire l'accès au système d'exploitation d'un ordinateur, il est bien connu que cette mesure de sécurité est insuffisante. Avec ou sans mot de passe, un voleur pourrait accéder au disque dur à l'aide d'une simple disquette de démarrage.

Le gestionnaire des opérations de services de réseau de la SCA a reconnu la nécessité d'une sécurité accrue. En plus d'émettre les directives précitées aux employés, il a informé le Commissariat que la SCA faisait des plans pour équiper tous ses ordinateurs, y compris les portatifs, d'un logiciel approprié de protection de l'ensemble des données stockées sur le disque dur.

Le Commissaire à la protection de la vie privée recommande fortement aux institutions fédérales de prendre toutes les précautions possibles pour protéger les données inscrites dans leurs ordinateurs portatifs. Si vous ne pouvez empêcher un voleur décidé de s'emparer de l'appareil, vous pouvez au moins vous assurer qu'il ne récoltera pas une grosse prime sous la forme de renseignements confidentiels utiles.

Destruction illégale et intentionnelle de documents

Pour que le Commissaire à la protection de la vie privée décide de porter directement ses conclusions à un sous-ministre, il faut qu'une question importante soit en jeu. Malheureusement, dans le cas présent, le sous-ministre en question n'entrevoyait pas la question sous le même angle.

En se penchant sur une plainte contre Revenu Canada, notre enquêteur avait pris des dispositions pour visiter le bureau régional du fisc. Sur place, il comptait interviewer plusieurs employés et inspecter les dossiers et documents appropriés. Son travail consistait à déterminer si Revenu Canada avait bien communiqué à une plaignante tous les renseignements personnels qu'elle avait demandés en vertu de la *Loi sur la protection des renseignements personnels*, et portant principalement sur une accusation de harcèlement.

Avant de se déplacer, notre enquêteur a contacté la coordonnatrice régionale des ressources humaines de l'endroit. Celle-ci lui a précisé que les dossiers recueillis à son intention incluaient des notes manuscrites d'un auteur inconnu, et qu'elle avait l'intention d'éliminer les doubles de documents. La coordonnatrice a cependant accepté la requête de notre enquêteur de ne pas purger les dossiers avant qu'il ne les ait revus.

Au cours de sa visite, notre enquêteur n'a pas retrouvé les notes manuscrites en question. Il a alors entrepris d'interviewer plusieurs des gestionnaires du bureau afin de découvrir ce qui s'était passé :

- La coordonnatrice des ressources humaines avait confié les dossiers de harcèlement à deux gestionnaires afin qu'ils y mettent de l'ordre et en fassent la chronologie.
- Un de ces deux gestionnaires a reconnu de lui-même avoir par la suite procédé à la destruction des notes manuscrites de l'enquêteur de la plainte de harcèlement, et ce tout en sachant pertinemment qu'une plainte en vertu de *la Loi sur la protection des renseignements personnels* était en cours et que ces notes relevaient d'une plainte antérieure en vertu de la même Loi.
- L'autre gestionnaire à qui on avait confié le dossier avait éliminé un autre jeu de notes manuscrites. Sans en garder copie au dossier, elle avait expédié ces notes manuscrites à leur auteur, soit à l'enquêteur d'une plainte antérieure de harcèlement déposée par la plaignante.

Comme notre enquête l'a montré, ces deux jeux de notes manuscrites avaient trait à certains éléments d'une enquête précédente qui auraient projeté une image négative du personnel local de l'endroit.

Les deux jeux de notes n'ont pas manqué à l'appel bien longtemps. D'un côté, notre enquêteur a persuadé l'auteur du deuxième jeu de notes de les restituer. De l'autre, un exemplaire du premier jeu de notes avait été conservé au siège social de Revenu Canada à Ottawa, probablement à l'insu du bureau régional. Éventuellement, le ministère a consenti à ce que les deux jeux de

notes soient remis au dossier d'enquête de harcèlement afin que la plaignante puisse y accéder à l'avenir.

Question résolue alors ? Pas tout à fait. Le problème de l'extraction et la destruction délibérées de dossiers par des représentants officiels restait entier. C'est ce point qui avait ébranlé le Commissaire et l'avait incité à porter le tout à l'attention du sous-ministre de Revenu Canada.

Plus précisément, le Commissaire s'inquiétait du geste « déplacé » et du comportement « répréhensible » de représentants de Revenu Canada qui avaient contrevenus aux dispositions de rétention et aux normes de destruction tant de la *Loi sur la protection des renseignements personnels* que de leur propre ministère. Les éléments de preuve en sa possession obligeaient le Commissaire à conclure que les responsables de Revenu Canada avaient délibérément tenté d'entraver son enquête.

Le sous-ministre a convenu que la destruction de renseignements personnels était une question sérieuse mais que le comportement de ses fonctionnaires n'avait rien de répréhensible puisqu'il était convaincu que ce déplorable incident n'était pas intentionnel et qu'il ne visait pas à nuire à l'enquête du Commissaire à la protection de la vie privée. Le sous-ministre ne s'est pas aventuré à préciser les éléments de preuve justifiant sa conviction.

Il a toutefois précisé qu'il rappellerait à ses fonctionnaires les pouvoirs et obligations du Commissaire à la protection de la vie privée et l'obligation qui leur incombe de respecter toutes les dispositions de la *Loi sur la protection des renseignements personnels*.

Le nouvel article 67.1 de la *Loi sur l'accès à l'information* interdit la destruction de documents sous peine d'amendes si cette destruction vise spécifiquement à empêcher l'accès aux documents en question. Nous regrettons que la *Loi sur la protection des renseignements personnels* ne contienne aucune disposition équivalente.

Rien ne vaut une explication claire

La faute n'en revient pas toujours aux ministères lorsqu'une demande d'accès à des renseignements personnels tarde à recevoir une réponse. À l'occasion, les demandes manquent elles-mêmes de précision et il revient aux employés des ministères de déterminer exactement ce que les requérants veulent. Et un requérant peut parfois éviter des semaines de retard grâce à un simple appel téléphonique.

Ainsi, un homme a récemment porté plainte à l'effet qu'un ministère tardait à répondre à sa demande d'accès en vertu de la *Loi sur la protection des renseignements personnels*. Sa demande visait tous les documents rajoutés à son dossier depuis sa « dernière demande ».

Aux yeux de l'agente responsable de l'accès à l'information et de la protection des renseignements personnels de ce ministère, cette nouvelle demande paraissait ambiguë. Elle croyait comprendre que le demandeur voulait copie des dossiers d'une enquête interne résultant de sa plainte de harcèlement contre certains responsables de l'organisme. Toutefois, la nouvelle demande identifiait certaines personnes étrangères à l'enquête et n'ayant donc pu être la source des documents demandés. En outre, l'individu avait déposé plusieurs demandes d'accès à ses renseignements dans le passé et la « dernière » en date n'avait rien à voir avec l'enquête en cours.

Bref, l'agente ne savait vraiment pas comment répondre à la nouvelle demande. Elle voulait bien y répondre mais manquait de renseignements pour procéder. Après plusieurs essais téléphoniques infructueux, elle a écrit au requérant pour lui demander de clarifier la nature exacte de sa « dernière demande », dont elle voulait le numéro de dossier.

Suite à cette lettre, le requérant a décidé de confier le tout à son avocat au lieu de répondre (par téléphone ou autre) à l'agente. Deux bonnes semaines plus tard, l'avocat communiquait avec le ministère et l'informait de son intention de porter plainte officiellement quant aux délais excessifs du traitement de la demande d'accès de son client. Expédiée formellement au Commissaire à la protection de la vie privée, cette lettre a été reçue comme une plainte officielle en vertu de la *Loi sur la protection des renseignements personnels*.

Cependant, l'intervention de l'avocat a contribué à accroître la confusion. En effet, en réponse à la question ayant trait à la « dernière demande », la lettre fournissait le numéro de dossier que l'agente du ministère jugeait encore ne pas être le bon. Cette dernière ignorait toujours la nature des documents visés par la demande.

L'article 13(2) de la *Loi sur la protection des renseignements personnels* précise que ceux qui demandent accès à des dossiers personnels en vertu de la Loi doivent fournir suffisamment de détails afin de permettre au ministère de retrouver l'information recherchée. En d'autres termes, il incombe à chaque requérant de s'assurer que sa demande n'est pas ambiguë.

Une longue conversation avec l'avocat a permis à notre enquêteur de

confirmer les soupçons de l'agente du ministère : les dossiers demandés avaient effectivement trait à l'enquête de harcèlement. L'enquêteur a indiqué à l'avocat que le numéro de dossier cité dans sa lettre de plainte n'avait rien à voir avec cette enquête. Bref, il y avait bel et bien eu confusion quant aux renseignements visés par le requérant, ce qui était pour le moins compréhensible.

L'avocat a finalement accepté de fermer le dossier en expédiant une lettre explicative au ministère.

Le Commissaire en a conclu que la demande du ministère pour des éclaircissements était justifiée et que la plainte de délai n'était pas fondée.

Question de patience...

Chapeau bas aux innombrables personnes du troisième âge qui connaissent et chérissent leurs droits à la vie privée.

Il s'agit ici du cas d'une québécoise qui en a eu assez de voir constater que n'importe qui pouvait lire son numéro d'assurance sociale à travers l'enveloppe de ses chèques de Sécurité de la vieillesse. Décidée à réagir, elle a porté plainte auprès du Commissaire à la protection de la vie privée. Après avoir enquêté, nous avons le plaisir de vous faire savoir que plus jamais cette personne ni ses semblables n'auront à subir ce type d'atteinte à leur vie privée.

Notre Commissariat n'aurait pas pu être davantage d'accord avec la plaignante lors de son enquête. Pourquoi en effet le NAS, ce numéro soi-disant confidentiel de tout citoyen canadien, apparaissait-il à la fenêtre des enveloppes expédiées par un ministère fédéral ? Ce n'était pas la première que cette question se posait. En fait, nous l'avons déjà soulevée à maintes autres reprises depuis 1986, alors que nous nous sommes penchés sur des plaintes tout aussi fondées que celle-ci.

Mais le problème était maintenant plus pressant. Pourquoi le personnel de Ressources humaines Canada contrevenait-il encore et toujours à la *Loi sur la protection des renseignements personnels* en divulguant des renseignements confidentiels sur ses enveloppes : le Commissariat ne lui avait-il pas souligné cette erreur à maintes reprises au cours des dernières années ? Le ministère ne l'avait-il pas à chaque fois reconnue, et promis de la régler ?

Pour être juste envers le ministère, cette fois la réponse a été différente —

plus de vaines promesses, plus de « l'année prochaine certainement », de question de « systèmes » ou de demi-mesures. Le ministère a non seulement dit qu'il enlèverait le NAS des chèques de sécurité de la vieillesse, mais il l'a fait, et ce dès le 1er novembre 1999.

C'est peut-être une toute petite victoire mais qui n'aurait jamais pu se concrétiser sans les protestations constantes des personnes âgées, dont la plaignante du Québec. Peut-être parce qu'elle comprend mieux la relation intégrale entre liberté et vie privée, la vieille génération a tendance à mal supporter les plus petites atteintes à l'une ou l'autre. La question maintenant est de savoir si la jeune génération compte relever le défi ?

Neuf moins trois font plus...pour notre vie privée !

Même s'il n'est pas visible par la fenêtre de l'enveloppe, le numéro d'assurance sociale imprimé sur un chèque du gouvernement ne demeure pas caché à jamais. Tôt ou tard l'enveloppe est ouverte, et le NAS peut être vu par des personnes aucunement concernées — notamment, par ceux ou celles qui encaissent le chèque.

Au cours des années, le Commissaire à la protection de la vie privée a reçu de nombreuses plaintes à cet effet. Lorsqu'il en a récemment reçu une d'une homologue nordique, cela a fait toute la différence.

La Commissaire à l'information et à la vie privée des Territoires du Nord-Ouest soutenait que Développement des ressources humaines Canada (DRHC) divulguait abusivement les numéros d'assurance sociale en les imprimant sur les chèques de prestations d'assurance emploi. Elle prétendait que les prestataires ne pouvaient pas, par conséquent, toucher leurs chèques sans révéler des renseignements personnels aux établissements financiers ou à tous les établissements qui acceptaient d'encaisser les chèques.

DRHC imprime encore le NAS sur plusieurs types de chèques. Le cas des chèques de prestations d'assurance emploi est peut-être celui que le Ministère défend le mieux. Dans le cas actuel, comme souvent par le passé, DRHC explique sa position comme suit :

- Vu que le NAS a été originellement conçu aux fins de l'assurance emploi, son utilisation sur les chèques d'assurance emploi est entièrement appropriée et valable. Par ailleurs, le NAS représente le numéro de dossier officiel dans le cadre du programme d'assurance emploi et, à ce titre, il constitue un élément important pour établir l'identité des bénéficiaires. Étant donné que de nombreuses personnes peuvent avoir

le même nom, les chèques d'assurance emploi ne sont pas émis à un nom, mais plutôt à un NAS.

- Il serait laborieux et coûteux de retrouver des chèques perdus ou volés en l'absence d'un NAS.
- En ce qui concerne la confidentialité, les établissements financiers utilisent déjà le NAS confidentiel pour effectuer d'autres transactions. Les autres établissements n'ont peut-être pas le même type de responsabilité concernant le NAS, mais les personnes qui décident d'y encaisser leurs chèques font un choix personnel.
- Les bénéficiaires ont aussi la possibilité de faire virer les chèques automatiquement dans leurs comptes bancaires. Le virement automatique constitue un autre moyen d'éviter que ne soit vu le NAS confidentiel.

Le Commissariat à la protection de la vie privée croit que l'argument de DRHC à une certaine valeur, surtout en ce qui a trait aux choix généralement accessibles aux bénéficiaires. En réalité, les établissements financiers accèdent déjà couramment au NAS, notamment pour effectuer des transactions comme la déclaration de revenus à Revenu Canada. Ils disposent aussi probablement de mesures pour protéger les renseignements personnels. De même, il est vrai que le virement automatique peut permettre d'assurer une plus grande confidentialité.

Cependant, dans le cas des Territoires du Nord-Ouest, la position de DRHC perd de la force. Dans les nombreuses régions peu peuplées du Nord canadien, les établissements financiers peuvent être peu nombreux et assez éparpillés. Que le chèque soit viré automatiquement ou non, il est déjà passablement difficile de se rendre à la banque. De nombreux habitants doivent pouvoir compter sur tout autre établissement en mesure d'encaisser des chèques comme, par exemple, le magasin général de l'endroit.

Naturellement, de tels établissements peuvent avoir de l'attrait, mais ils n'ont pas la réputation d'offrir le genre d'anonymat auquel on s'attend souvent dans un établissement financier. Après tout, c'est une chose que de voir un caissier de banque impartial parcourir votre NAS des yeux. Mais être obligé de divulguer des renseignements personnels à un ami, un parent, un voisin ou une connaissance locale, c'est là une toute autre histoire.

Le Commissariat est heureux d'annoncer qu'à la suite des discussions en rapport direct avec la plainte venue des Territoires du Nord-Ouest, DRHC a assoupli sa position. Le Ministère a consenti à se pencher sur l'utilisation des numéros d'assurance sociale figurant sur les chèques — non seulement dans

les cas de l'assurance emploi, mais dans le cadre de *tous* ses programmes. De façon plus concrète, le Ministère a déjà proposé des changements. En effet, au lieu d'imprimer le NAS en entier, le Ministère n'imprimerait que les six derniers chiffres sur chacun des chèques émis.

Six chiffres suffiraient-ils à DRHC ? Oui. Le Ministère a dit n'avoir besoin que de six chiffres pour faire la plupart des identifications. Mais la simple élimination de trois chiffres du NAS peut-elle régler la question de la confidentialité ? Cela suffira en grande partie. D'une part, les six chiffres restants ne seraient ni assimilés comme faisant partie d'un NAS ni reconnaissables comme tels. D'autre part, personne, pas même DRHC, ne pourrait deviner ou recréer le NAS complet à partir des six derniers chiffres.

Bref, tant le Commissaire fédéral que son homologue territoriale considèrent que la proposition constitue un compromis raisonnable. Bien qu'il reconnaisse que le changement ne se produira pas du jour au lendemain, le Commissaire fédéral a assuré à sa collègue des Territoires du Nord-Ouest qu'il surveillera l'évolution de ce dossier.

Demandes de renseignements

Après une brève accalmie, le nombre de demandes de renseignements a de nouveau monté en flèche cette année. Nos deux employés préposés au traitement des demandes de renseignements ont répondu à quelque 11 256 appels et lettres en 1999-2000. Ce chiffre dépasse de 953 le total de l'an dernier, et de 925 celui de 1997-1998.

Le tableau suivant classe les demandes de renseignements reçues en grandes catégories.

Demandes de renseignements par catégorie

pour l'exercice financier prenant fin le 31 mars 2000

Acheminées ailleurs	135
Acheminées à un autre organisme fédéral	686
Acheminées aux commissaires provinciaux	794
Adoption, généalogie, personnes portées disparues	83
Affaires publiques (médias, publications)	1036
Aucune compétence fédérale	805
Aucune compétence, secteur privé (Loi C-6)	780
Autres	698
Dossiers criminels, pardons, dérogations américaines	130
Institutions financières, assurance, bureaux de crédit	367
Loi, interprétation & application	4364
Marketing direct	83
Médical	121
Numéro d'assurance sociale	1099
Télécommunications	75
Total	**11 256**

Faits particulièrement intéressants

Renseignements publics : Plus de gens que jamais ont signalé qu'ils avaient de la difficulté à trouver des formulaires de demande d'accès à des renseignements personnels et des exemplaires d'*InfoSource*, catalogue des

fonds de renseignements du gouvernement fédéral. Le Secrétariat du Conseil du Trésor est tenu par la *Loi sur la protection des renseignements personnels* de produire ces documents et d'en distribuer des copies aux bureaux de poste, bibliothèques et autres lieux publics. Cependant, le Conseil du Trésor semble devenir de moins en moins diligent à cet égard — du moins en ce qui concerne la distribution. Selon les gens qui nous ont appelés, non seulement bien des bureaux de poste ne disposent pas de ces documents, mais certains employés des Postes, surtout dans les petits points de vente, ne savent même pas qu'ils existent.

De plus, même lorsqu'ils trouvent des exemplaires d'*InfoSource*, les gens apprécient rarement ce qu'ils voient. Ce catalogue suscite un manque de satisfaction qui se traduit par de nombreux appels de plainte au Commissariat. Les plaignants considèrent qu'*InfoSource* est trop gros et difficile à manipuler, trop technique, trop difficile à lire, et qu'il est difficile de s'y retrouver — en résumé, il est bien loin d'être aussi utile et convivial qu'il devrait l'être pour un citoyen canadien moyen. Et le personnel du Commissariat, qui consulte ce catalogue chaque jour, ne peut qu'être d'accord. Le répertoire des sources d'information du gouvernement fédéral devrait être davantage un guide pour l'utilisateur moyen qu'un recueil exhaustif.

Le Commissariat aimerait aider à améliorer *InfoSource* et, à cette fin, il a déjà engagé des discussions avec le Conseil du Trésor.

Numéros d'assurance sociale : Une fois encore, le NAS a fait l'objet de nombreuses demandes de renseignements. Le nombre de demandes liées au NAS présentées cette année a même dépassé le total de l'an dernier, qui avait pourtant connu une hausse importante à la suite des commentaires du Vérificateur général. En fait, plus de 40 p. 100 des demandes de renseignements présentées par téléphone en 1999-2000 avaient trait à l'utilisation du NAS.

Surveillance électronique : Beaucoup de gens ont posé des questions au sujet de la légalité de diverses formes de surveillance électronique, notamment les caméras cachées et la surveillance des appels téléphoniques et de l'utilisation d'ordinateurs. Parmi les personnes qui nous ont téléphoné, il y avait des employés qui étaient sous surveillance et des employeurs qui envisageaient de surveiller leur milieu de travail.

Données des recensements effectués après 1911 : Le Commissariat a encore reçu des demandes de renseignements au sujet de la communication des résultats du recensement de 1911 et des recensements subséquents. La

plupart de ces demandes ont été présentées en réaction à l'opposition qu'a exprimée le Commissaire à la protection de la vie privée face à la proposition de communiquer des renseignements dont le gouvernement s'est pourtant engagé à assurer la confidentialité.

Statistique Canada : L'Enquête sur la population active a provoqué de nombreuses plaintes au sujet du personnel de Statistique Canada que beaucoup de gens ont accusé de les harceler. La prochaine enquête importante de 2001 devrait aussi susciter un nouveau flot de demandes de renseignements relativement au comportement des sondeurs et à l'obligation des citoyens de répondre ou non à leurs questions.

Secteur privé : Chaque année, nos employés répondent à un grand nombre de demandes de renseignements concernant les entreprises et les institutions du secteur privé. Cette année, par exemple, beaucoup de gens se sont de nouveau dits insatisfaits du processus mis en place par les institutions financières pour régler les plaintes de leurs clients. D'autres ont allégué que les bureaux de crédit fournissent des renseignements erronés ou inexacts sur eux, ou que des agences de recouvrement les harcèlent et communiquent leurs renseignements personnels à des tiers. Plusieurs appels émanaient d'employés du secteur privé qui essayaient d'obtenir un accès à leurs dossiers personnels. Ces personnes ont été invariablement choquées d'apprendre qu'aucune loi ne permettait actuellement un tel accès.

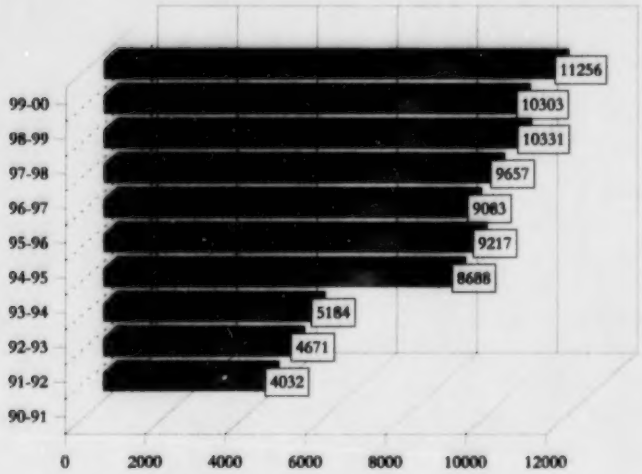
Jusqu'ici, avec pour seule ligne directrice la *Loi sur la protection des renseignements personnels*, le Commissariat à la protection de la vie privée s'est vu limité dans ses réponses. Avec l'adoption de la Loi C-6, toutefois, nous espérons devenir beaucoup plus utiles à ces personnes.

Pendant le mandat du Commissaire

En dix ans de service, le Commissaire Phillips a vu le nombre annuel de demandes de renseignements presque tripler, passant de 4 032 en 1990-1991 à 11 256 en 1999-2000. L'augmentation annuelle moyenne s'élève à près de 10 p. 100, et le nombre total de demandes de renseignements reçues depuis 10 ans s'élève à 82 422.

Le tableau qui figure ci-dessous indique les totaux de demandes de renseignements personnels de chacune des dix années de service du Commissaire.

Demandes de renseignements 1990-2000



Les dix ministères les plus visés

pour l'exercice financier prenant fin le 31 mars 2000

	Total	Accès	Délais	Vie Privée	Autres
Service correctionnel Canada	316	109	136	71	
Revenu Canada (maintenant Agence des douanes et du revenu du Canada)	231	103	81	47	
Défense nationale	189	53	91	45	
Gendarmerie royale du Canada	130	67	37	26	
Développement des ressources humaines Canada	120	35	16	69	
Commission d'appel de l'immigration	108	8	92	8	
Citoyenneté et immigration Canada	72	32	29	11	
Justice, Ministère de la	64	52	3	9	
Service canadien du renseignement de sécurité	58	53	3	2	
Société canadienne des Postes	38	10	3	25	
Autres	260	124	66	69	1
Total	**1586**	**646**	**557**	**382**	**1**

Plaintes réglées par institution et résultats

pour l'exercice financier prenant fin le 31 mars 2000

Institution	Fondée	Fondée; Résolue	Non fondée	Abandonnée	Résolue	Réglée	Total
Affaires indiennes et du Nord Canada	2	1	1	0	0	1	5
Affaires étrangères et Commerce int.	4	0	4	0	0	2	10
Agence de promotion économique du Canada Atlantique	0	0	1	1	0	0	2
Agence spatiale canadienne	0	1	3	0	0	0	4
Agriculture et Agro-alimentaire Canada	4	0	0	0	0	1	5
Sous-total	10	2	9	1	0	4	26

Institution	Fondée	Fondée; Résolue	Non fondée	Aban-donnée	Résolue	Réglée	Total
Anciens combattants Canada	5	1	5	1	1	5	18
Archives Nationales du Canada	3	3	4	0	0	7	17
Banque fédérale de développement du Canada	0	0	0	0	0	1	1
Bureau de l'Inspecteur général du SCRS	0	0	0	0	2	0	2
Bureau du Conseil Privé	0	0	3	0	1	1	5
Bureau du Directeur général des élections	0	0	0	0	1	0	1
Citoyenneté et immigration Canada	41	8	10	4	1	11	75
Com. des plaintes du public contre la GRC	0	0	0	0	0	3	3
Com. de l'immigration et du statut du réfugié	90	15	11	1	0	0	117
Com. canadienne des droits de la personne	0	0	0	0	0	1	1
Commission nationale des libérations conditionnelles	1	4	10	1	4	3	23
Commission d'appel des pensions	0	0	0	0	0	1	1
Commission des relations de travail dans la Fonction publique	0	0	1	0	0	0	1
Commission de la Fonction publique	12	1	0	1	0	4	18
Conseil du Trésor du Canada	0	0	3	0	0	0	3
Conseil national de recherches Canada	0	0	1	0	0	0	1
Conseil de la radiodiffusion et des télécommunications canadiennes	0	0	1	0	0	0	1
Défense Nationale	107	10	43	5	3	28	196
Développement des ressources humaines Canada	14	3	21	9	2	50	99
Sous-total	283	47	122	23	15	119	609

Institution	Fondée	Fondée; Résolue	Non fondée	Aban-donnée	Résolue	Réglée	Total
Environnement Canada	0	0	2	0	0	0	2
Gendarmerie royale du Canada	19	3	42	8	3	31	106
Industrie Canada	1	0	0	0	0	0	1
Justice, Ministère de la	1	3	15	2	1	14	36
Ministère du Patrimoine canadien	2	0	2	0	1	1	6
Musée canadien des civilisations	0	0	0	0	0	1	1
Pêches et Océans	0	0	1	0	0	0	1
Ressources naturelles Canada	2	0	3	2	0	1	8
Revenu Canada (maintenant Agence des douanes et du revenu du Canada)	93	8	41	6	4	28	180
Santé Canada	4	1	6	4	1	2	18
Service correctionnel Canada	149	13	71	15	7	45	300
Service canadien du renseignement de sécurité	3	0	15	0	0	18	36
Société canadienne des Postes	6	1	7	6	1	15	36
Société canadienne des Ports	1	1	0	0	0	1	3
Société du crédit agricole Canada	0	0	0	1	0	0	1
Solliciteur général Canada	0	1	13	0	0	1	15
Statistiques Canada	0	0	0	3	0	0	3
Transports Canada	7	1	2	2	0	1	13
Travaux publics et Services gouv. Canada	11	2	6	0	0	5	24
Total	**582**	**81**	**348**	**72**	**33**	**283**	**1399**

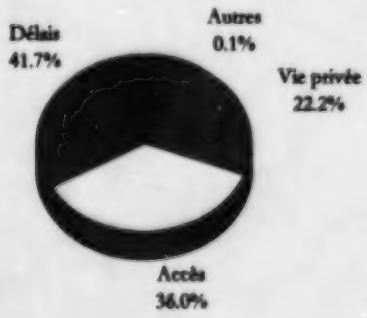
Origine des plaintes réglées

pour l'exercice financier prenant fin le 31 mars 2000

Terre-Neuve	3
Île-du-Prince-Édouard	6
Nouvelle-Écosse	43
Nouveau-Brunswick	45
Québec	337
Région de la capitale nationale - Québec	9
Région de la capitale nationale - Ontario	192
Ontario	327
Manitoba	72
Saskatchewan	40
Alberta	85
Colombie-Britannique	229
Territoires du Nord-Ouest	1
Yukon	2
Hors Canada	8
Total	**1399**

Plaintes réglées par motif

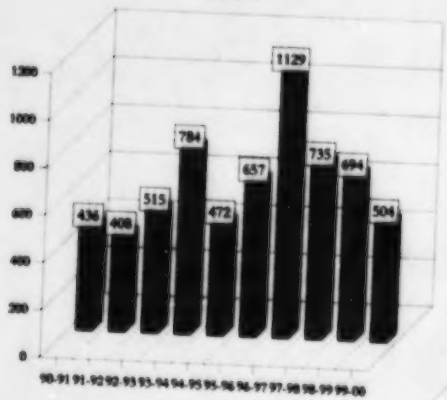
Exercice financier 1999-2000



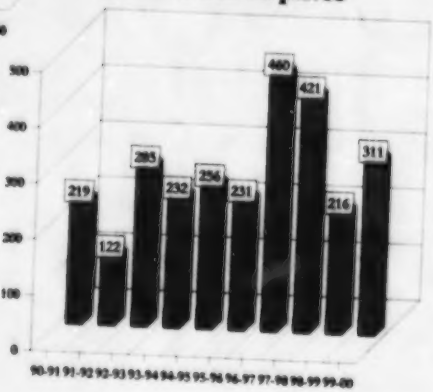
Plaintes réglées par motif

pour les dix dernières années

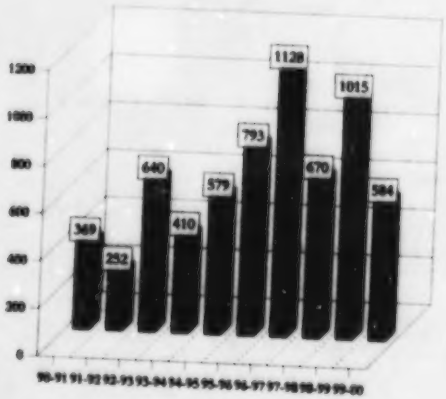
Accès



Atteintes à la vie privée



Délais



Devant les tribunaux

Leçons des dix dernières années

Il nous a paru utile de récapituler les principaux enseignements que nous avons tirés des décisions rendues par les tribunaux ces dix dernières années, et citées à la fin de cette section du rapport annuel.

Accès aux renseignements personnels

- Lorsqu'il reçoit une demande de communication de renseignements personnels en vertu des dispositions d'intérêt public de la *Loi sur la protection des renseignements personnels*, le responsable d'un organisme fédéral doit vérifier si l'intérêt public invoqué justifie suffisamment les atteintes à la vie privée qu'engendrerait la communication. Si le responsable s'y applique correctement, les tribunaux respecteront sa décision (C).
- Les renseignements reliés à un poste fédéral (*p. e.* sa cote sécuritaire, sa classification ou ses exigences linguistiques) ne sont pas « personnels », même lorsqu'ils révèlent accidentellement certaines choses au sujet des employés occupant ces postes (C & I). Par contre, les renseignements reliés à ces employés (*p. e.* leur solde de congés, leur état de santé ou leur rendement professionnel) sont « personnels » (C & J).
- Le droit d'une personne d'accéder à ses renseignements personnels n'est pas absolu si ces derniers sont tellement mélangés à ceux d'un autre individu que la communication à la première personne révélerait certaines choses au sujet de l'autre individu (D).
- Toutes les parties impliquées dans une enquête administrative (découlant *p. e.* d'une plainte de harcèlement ou d'un grief) devraient pouvoir accéder à tout renseignement ayant mené à la décision finale. Une telle communication est jugée compatible par la *Loi sur la protection des renseignements personnels* et répond aux impératifs de la justice naturelle (F).

Contrôle des renseignements personnels

- Tous les renseignements détenus par un organisme fédéral sont assujettis à la *Loi sur la protection des renseignements personnels*, à l'exception des renseignements qui sont spécifiquement exclus de son application. Rien dans la *Loi* n'indique que ce contrôle peut être réduit ou laissé de côté dans le cas d'un contrat passé avec une tierce partie (G).

Lien entre la *Loi sur la protection des renseignements personnels* et la *Loi sur l'accès à l'information*

- La *Loi sur la protection des renseignements personnels* est tout aussi importante que la *Loi sur l'accès à l'information* et doit recevoir la même considération lorsqu'il s'agit de renseignements détenus par le gouvernement. Toutefois, si ces renseignements sont « personnels » au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, la protection de la vie privée prime tout droit d'accès à ces renseignements (C).

Secret professionnel des avocats

- Seul le client, et non l'avocat, a le droit de renoncer à la protection qui s'applique aux communications entre ces deux personnes — autrement dit le secret professionnel qui les lie (A).
- L'abandon du secret professionnel quant à une partie d'un document et la divulgation de cette dernière ne signifie pas automatiquement que le reste du document doit être également communiqué. Toutefois, l'ensemble du document pourrait devoir être communiqué s'il s'avère que la divulgation partielle initiale avait pour but d'induire le destinataire des renseignements en erreur (B).
- Le détail des honoraires d'un avocat est protégé par le secret professionnel puisqu'il peut révéler la nature du travail accompli pour le compte du client (B).
- Vu donné son absence de la *Loi sur la protection des renseignements personnels*, la définition du secret professionnel se trouve dans le *common law* (H).
- Tout responsable d'un organisme fédéral choisissant de ne pas communiquer certains renseignements au nom du secret professionnel doit pouvoir prouver que chacun des documents refusés est un avis juridique ou a été préparé dans l'optique principale d'un litige (H).
- Avant de refuser de communiquer certains renseignements au nom du secret professionnel, le responsable d'un organisme fédéral doit confirmer que le secret s'applique bel et bien aux documents visés, et que le client refuse de renoncer au secret (E).

Arrêtés cités ci-dessus :

A. R. c. Campbell [1999] R.C.S. 565 ;

B. Stevens c. Canada (Bureau du Conseil privé) (1997) 144 D.L.R. (4ième) 553 ;

C. Dagg c. Canada (Ministre des Finances), [1997] 2 R.C.S. 403 ;

D. Mislan c. Canada (Ministre du Revenu), T-2790-96, arrêté du 22 mai 1998, C.F. (1re inst.), sans compte rendu ;

E. Congrès juif canadien c. Canada (ministre de l'Emploi et de l'Immigration) [1996] 1 C.F. 268 (1re inst) ;

F. Puccini c. Canada (Directeur général, Services de l'administration corporative, Agriculture Canada), [1993] 3 C.F. 557 ;

G. Société canadienne des postes c. Canada (Ministre des Travaux publics [1993] 3 C.F. 320)(1ère inst.); confirmée à (1993) 64 F.T.R. 62 (C.A.F.) ;

H. Weiler c. Canada (Ministre de la Justice) [1991] 3 C.F. 617 (1re inst.) ;

I. Canada (Commissaire à l'information) c. Secrétaire d'État aux Affaires extérieures [1990] 1 C.F. 395 ;

J. Canada (Commissaire à l'information) c. Canada (Solliciteur général) [1988] 3 C.F. 551.

Dossiers actifs

- le Commissaire à la protection de la vie privée c. le Procureur général du Canada (Dossier de Cour : A-121-99)
- le formulaire E-311 (Dossier de Cour : A-401-99)

Ces deux litiges contestaient l'utilisation par Développement des ressources humaines Canada (DRHC) des déclarations de douane des voyageurs revenant au Canada (formulaires E-311). DRHC recourt à ces déclarations pour vérifier l'admissibilité aux prestations d'assurance emploi (AE). Le premier litige était un appel de la décision de la juge Tremblay-Lamer, laquelle portait sur l'interprétation tant de l'alinéa 108(1)b) de la *Loi sur les douanes* (pouvoir du ministre des Douanes d'autoriser des communications de renseignements) que du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels* (la *LPRP*). La Cour d'appel a rendu ses deux décisions le 9 février 2000.

La Juge Tremblay-Lamer avait décidé que le ministre du Revenu avait, en autorisant de façon générale la divulgation des formulaires E-311 le 26 juillet 1991, mal exercé son pouvoir discrétionnaire parce qu'il l'avait compromis pour l'avenir et parce qu'il avait pris sa décision en se basant sur des considérations non pertinentes. La Cour d'appel a cependant décrété que « la question qui avait été posée à la juge Tremblay-Lamer n'avait rien à voir avec cette autorisation générale, mais avec le protocole d'entente ancillaire

concernant la collecte et la communication de renseignements recueillis par les douanes sur les voyageurs daté du 26 avril 1997 entre Revenu Canada, d'une part et la Commission de l'assurance emploi, d'autre part » [traduction]. Selon la Cour d'appel, le protocole d'entente d'avril 1997 est en soi une autorisation ministérielle indépendante de celle de 1991.

La Cour d'appel a également statué que l'alinéa 8(2)b) de la *LPRP* (qui permet la communication de renseignements personnels si celle-ci est prescrite par une autre loi ou ses règlements) devait être interprété libéralement : « Dans ce contexte, l'alinéa 8(2)(b) ne peut s'interpréter que comme permettant au Parlement de conférer à un ministre (par exemple) par le biais d'une loi une grande marge de manœuvre, tant sur la forme que sur le fonds, quant à la communication de renseignements que son ministère a recueillis, cette liberté devant toutefois s'exercer dans le respect des objectifs de la *LPRP*. » [traduction]

La Cour d'appel a conclu que ces objectifs avaient été respectés par la ministre parce que « cette dernière s'est assurée que la communication demandée par la Commission de l'assurance emploi était permise et qu'elle serait limitée aux seuls renseignements requis par la Commission » [traduction]. De plus, le protocole d'entente daté d'avril 1997 incluait des restrictions quant à l'utilisation de ces renseignements et de leur communication à des tiers, ainsi que le besoin d'une journalisation et de la destruction des renseignements.

Le second litige tentait de décider si les prestataires de l'AE et le reste des Canadiens peuvent raisonnablement s'attendre à ce que les renseignements qu'ils fournissent sur les formulaires E-311 restent confidentiels. Le cas échéant, cette attente est-elle suffisante pour faire intervenir les mécanismes de protection de l'article 8 de la *Charte canadienne des droits et libertés* ? Le litige portait aussi sur la possibilité que l'alinéa 32(b) de la *Loi sur l'assurance emploi* constitue une entrave à la liberté de circulation garantie par le paragraphe 6(1) de la *Charte*. La Cour d'appel a répondu à ces questions par la négative.

Le Commissaire à la protection de la vie privée va demander à la Cour Suprême la permission d'interjeter appel de ces décisions. Si l'interprétation que la Cour d'appel a faite de l'alinéa 8(2)(b) de la *LPRP* est la bonne, cela signifie que cet alinéa n'offre aucune protection aux Canadiens contre la communication de leurs renseignements par un organisme fédéral dont la loi habilitante permet à son ministre d'en décider à sa guise en la matière. Quelque vague que ce soit l'article 108 de la *Loi sur les douanes* (ou toute autre disposition comparable d'une autre loi), il aurait alors préséance sur la *LPRP*.

Le Commissaire croit qu'une fouille électronique de bases de données fédérales fait fi tant des protections qu'offre la *Charte* contre les fouilles ou les saisies abusives que de la présomption d'innocence — surtout lorsqu'une telle fouille ne repose sur aucun soupçon raisonnable et n'est sujette à aucune révision indépendante. Si de tels couplages devenaient chose courante, le gouvernement ne protègerait plus la confidentialité d'aucun des renseignements personnels des citoyens (sauf dans certains cas clairement définis par la loi), et ce que ces renseignements aient été fournis de plein gré ou sous la contrainte. Si l'alinéa 8(2)(b) de la *LPRP* n'existe que pour permettre n'importe quelle communication de renseignements désirée par le gouvernement, et si la *Charte* n'offre aucune protection contre de tels couplages de renseignements personnels, plus rien n'empêchera alors le gouvernement de compiler et de partager — y compris à l'extérieur du fédéral — d'énormes bases de données sur chacun de nous.

La plupart des lois actuelles protégeant la vie privée des citoyens de divers pays sont axées sur des pratiques équitables en matière de gestion de l'information. Ces pratiques limitent notamment la collecte de renseignements personnels, et restreignent leur utilisation et leur communication aux fins pour lesquelles ils ont été recueillis. La *LPRP* édicte elle aussi de telles pratiques. Bien qu'il existe certaines exceptions à ces dernières (tel le paragraphe 8(2) de la *LPRP*, ces exceptions doivent généralement être aussi peu nombreuses et avoir un impact aussi limité que possible. Le Commissaire croit que la Cour d'appel vient d'élargir la portée du paragraphe 8(2) à un point tel que les protections offertes par la *LPRP* ne sont plus que symboliques.

- le Commissaire à la protection de la vie privée c. le Conseil canadien des relations de travail (Dossier de cour : A-685-96)

Tel qu'indiqué dans notre rapport annuel 1996-97 (à la page 47), le Commissaire à la protection de la vie privée a interjeté appel de cette décision. L'audition de la cause est prévue pour le 9 mai 2000.

- Robert Lavigne c. le Commissaire aux langues officielles et le Commissaire à la protection de la vie privée (intervenant) (Dossier de cour : A-678-98)

Tel qu'indiqué dans notre dernier rapport annuel (à la page 92) le Commissaire aux langues officielles a interjeté appel de cette décision mais la Cour d'appel est débordée. Cette cause pourrait devoir attendre à l'automne 2000 avant d'être entendue.

Coup de pouce à la Loi C-6

La technologie à l'aide de notre vie privée sur l'Internet

Ceux qui ont lu les rapports annuels précédents se rappellent peut-être nos récriminations au sujet de l'érosion de la protection des renseignements personnels sur l'Internet : courriel non protégé, « cookies » omniprésents, anciens commentaires qui reviennent nous hanter — la liste était longue et s'allongeait chaque année. L'Internet n'est plus la tribune d'échange entre universitaires qu'il a déjà été. Il est maintenant bien ancré dans le monde des affaires. Presque tous les propriétaires d'un site Web ont des visées pécuniaires, ce qui donne lieu à de nouvelles stratégies visant à attirer, à retenir, à suivre, à étudier, à cibler et, quelquefois, à écarter ou à rejeter certains internautes.

Jusqu'à tout récemment, ces derniers ne savaient que peu de choses, voire rien du tout, sur ce suivi de leurs gestes par les propriétaires de sites Web. Cependant, l'intérêt grandissant des médias pour le commerce électronique et les pirates informatiques ont rendu les internautes, des novices aux pros, plus judicieux dans la communication de leurs renseignements personnels via l'Internet. De plus, certaines entreprises ont commencé à développer et à exploiter un marché prometteur de produits visant à améliorer la vie privée des internautes. Certains doivent être installés directement sur le disque dur de votre ordinateur personnel. D'autres sont offerts sur le Web. Certains sont résumés plus bas.

Le Commissariat à la protection de la vie privée répète depuis longtemps qu'il n'existe pas de meilleur remède aux collectes et aux utilisations abusives de renseignements personnels qu'une bonne loi sur la protection de la vie

privée, ce que la Loi C-6 devrait accomplir. Cependant, tout comme les lois actuelles n'empêchent pas les gens de prendre des cours d'autodéfense ni de faire installer des verrous à leurs portes, les internautes peuvent recourir à certaines technologies pour encore mieux se protéger dans le cyberespace. Évidemment, ces produits ne remplacent pas la vigilance de l'utilisateur, mais ils peuvent certainement rassurer les internautes qui tiennent à ce que leurs renseignements restent confidentiels.

Navigation, groupes de discussion et de nouvelles

L'un de ces produits, *Freedom*, logiciel commercial de Zero Knowledge conçu pour rouler sur votre ordinateur, a été lancé récemment. *Freedom* permet aux mordus de l'Internet de naviguer sous divers noms d'emprunt (un *nom de Net*, si vous voulez) : un pour les sites relatifs à l'immobilier, un autre pour les sites de recherche sur le cancer, un troisième pour les sites de courses de chevaux, etc. Même si un site Web peut quand même suivre les gestes de votre pseudonyme et même lui envoyer un « cookie », les propriétaires du site ne sauront jamais qui se cache derrière le nom de LoupGarou ou BellePrincesse. De plus, les abonnés de *Freedom* peuvent utiliser des noms d'emprunt lorsqu'ils participent à un groupe de discussion ou de nouvelles. SiegeSoft vient tout juste de lancer un produit semblable, mais qui est quant à lui disponible du Web.

Mais ce genre de logiciel n'est pas nouveau : The Anonymizer, site commercial bien connu, offre aux utilisateurs la possibilité de naviguer sur le Web et de s'abonner à des groupes de nouvelles de façon anonyme, et ce, depuis plusieurs années. Privada Inc. offre également un moyen commercial de naviguer de façon anonyme sur le Web, mais, contrairement à Zero Knowledge et The Anonymizer, l'entreprise peut relier un nom d'emprunt à l'identité réelle d'une personne si quelqu'un le lui demande — par exemple, un organisme d'application de la loi. En septembre 1999, PrivacyX a lancé un service concurrentiel de navigation et de courriel anonymes, mais elle a annulé l'option navigation quelques jours plus tard à cause d'une lacune décelée dans le logiciel.

En octobre 1999, Eponymous a commencé à offrir aux internautes un utilitaire gratuit qui sépare les données identifiant les internautes de leurs autres renseignements personnels comme l'âge, le sexe, les intérêts et les désirs. L'entreprise prévient également les internautes des pratiques de chaque site en matière de renseignements personnels. Lorsqu'un site présente un formulaire d'inscription, le dispositif fournit les données demandées, sauf celles identifiant l'internaute. En octobre également, Lucent Technologies a lancé Proxymate, dispositif gratuit qui permet aux utilisateurs de bloquer l'information habituellement transmise aux sites Web et de créer des noms

d'emprunt pour s'inscrire aux sites.

Courriel

Les services de courriel anonyme transmettent un message à son destinataire après avoir enlevé tous les renseignements identifiant l'expéditeur. Cependant, ces services peuvent être obligés de dévoiler l'identité de certains de leurs clients. Il semblerait même que certains organismes gouvernementaux ou que certaines autorités policières exploitent de tels services. La meilleure solution de rechange aux services de courriel anonymes est le cryptage — plus il y a de bits dans les clés de cryptage, meilleure... mais plus lente... est la protection.

Pretty Good Privacy, logiciel de Phil Zimmerman maintenant distribué par Network Associates, est l'un des logiciels de cryptage de courriel les mieux connus des utilisateurs d'ordinateurs personnels, même si certains utilisateurs pourraient le trouver trop complexe à leur goût. *Freedom* de Zero Knowledge, permet aux abonnées d'envoyer et de recevoir des messages chiffrés non repérables (à l'aide de clés de 2 048 bits) par l'entremise d'une série d'ordinateurs situés un peu partout dans le monde.

Même si PrivacyX a hélas dû annuler son produit de navigation anonyme, l'entreprise offre toujours aux abonnés un service de courriel anonyme. ZipLip, disponible sur le Web, permet de chiffrer les messages à l'aide de clés de 128 bits et de « déchiqueter » automatiquement ces derniers une fois lus, ne laissant ainsi aucune trace de votre correspondance. Plus souple, mais fonctionnant selon le même principe, le logiciel 1on1 de Global Market offre des messages chiffrés à l'aide de clés de 2 048 bits et permet aux utilisateurs de préciser la date à laquelle un message devrait être détruit. (Dans les faits, le message n'est jamais vraiment effacé : c'est le mot de passe de décryptage joint au message qui cesse d'être valide.) Le service *Interosa* de QVtech est encore plus souple : il permet d'envoyer un message chiffré et de préciser plusieurs aspects de son usage, notamment l'identité des personnes à qui on peut le faire suivre et les options d'impression, d'édition ou de copie. Le message peut également être effacé du serveur *Interosa* après une date spécifiée.

Pour terminer la liste des technologies protégeant votre vie privée sur l'Internet, mentionnons HushMail, service Web gratuit de cryptage complet de messages (clés de 1 024 bits). Enfin, le produit de Tumbleweed Communications Inc. permet au destinataire d'un message de se rendre sur le site de l'expéditeur pour visualiser ou récupérer un message ou un document chiffré par l'entremise d'une page Web protégée à laquelle seul le destinataire a accès.

L'Association canadienne du marketing veut protéger les enfants

Le Commissariat à la protection de la vie privée recommande depuis de nombreuses années l'adoption d'une loi pour protéger la vie privée de la population canadienne lorsque celle-ci transige avec le secteur privé. La Loi C-6 répond donc à nos attentes, mais nous reconnaissons également l'importance de mesures complémentaires telles la vigilance des consommateurs ou le recours à des technologies protégeant notre vie privée (voir plus haut). Ces mesures complémentaires comprennent également les efforts déployés par certaines entreprises pour protéger la vie privée de leurs clients.

L'Association canadienne de marketing (ACM) est reconnue pour avoir déployé de tels efforts à plusieurs occasions. Elle a été l'une des premières associations industrielles d'importance au Canada à imposer à ses membres un code d'éthique en matière de vie privée et à demander au gouvernement fédéral de légiférer pour l'ensemble du secteur privé. L'an dernier, l'ACM créait un autre précédent : elle présentait ses lignes directrices régissant le marketing destiné aux enfants. On peut trouver ces lignes directrices dans le *Code de déontologie et Normes de pratiques* (le « Code ») de l'ACM dans la section des « Considérations spéciales se rapportant au marketing destiné aux enfants ».

Selon ces lignes directrices, un enfant est une personne qui n'a pas encore célébré son 13e anniversaire. Lorsqu'ils élaborent des programmes de marketing destinés aux enfants, les spécialistes en marketing doivent observer les principes suivants :

- emploi de « techniques de marketing appropriées pour les enfants ». Ces techniques consistent entre autres à utiliser des termes faciles à comprendre pour les enfants et à ne pas adopter de pratiques susceptibles d'exploiter « la crédulité des enfants, leur manque d'expérience ou leur sens de la loyauté » ;obtention du « consentement exprès » du parent ou du tuteur de l'enfant avant de recueillir, de conserver ou de communiquer des renseignements personnels sur celui-ci ;
- refus d'honorer une commande provenant d'un enfant sans le consentement exprès d'un parent ou d'un tuteur.

Les enfants sont particulièrement réceptifs aux techniques de marketing et sont donc des cibles faciles à exploiter à des fins commerciales. On entend souvent parler de cas où des enfants ont, sans le savoir, communiqué des

renseignements sur eux ou d'autres membres de leur famille à des spécialistes en marketing sans vergogne. Il est donc nécessaire d'élaborer des considérations spéciales se rapportant au marketing destiné aux enfants et, à cette fin, l'initiative de l'ACM arrive à point nommé.

Les lignes directrices de l'ACM ne précisent pas de quelle façon ces principes doivent être appliqués dans l'« environnement virtuel » du marketing en ligne. Nous ignorons comment un spécialiste en marketing déterminera ou confirmera l'âge d'un individu. Il sera également difficile de vérifier l'authenticité des dires d'une personne qui déclare être le parent ou le tuteur d'un enfant afin de répondre à une demande de renseignements ou d'accepter une commande. Voilà quelques-uns des problèmes auxquels se butent les responsables des services américains de courriel et de sites Web pour tenter de respecter leur *Children's Online Privacy Protection Act*, laquelle exige des spécialistes en marketing qu'ils obtiennent le consentement d'un parent avant de recueillir, d'utiliser ou de communiquer des renseignements personnels fournis par un enfant.

Le Code de l'ACM prévoit que, lorsque les spécialistes en marketing recueillent auprès des consommateurs des renseignements personnels qui peuvent être liés aux données d'activité fournies par un internaute lors de sa visite d'un site Web, les consommateurs doivent être informés du genre de renseignements recueillis et de la façon dont ils seront utilisés. De plus, on est censé leur donner la réelle possibilité de refuser que ces renseignements soient recueillis ou communiqués à des fins de marketing. Le Code de l'ACM indique également qu'il incombe au consommateur d'exercer son droit de faire supprimer des renseignements qui permettent de l'identifier, une responsabilité déraisonnable à nos yeux, surtout lorsqu'il s'agit d'enfants.

Selon l'ACM, cependant, le meilleur moyen de contrer l'abus des enfants sur l'Internet reste l'éducation. À cet égard, les lecteurs sont invités à consulter la publication de l'ACM intitulée *Comment protéger la vie privée des enfants à l'ère de l'information : Conseils à l'intention des parents*, à l'adresse http://www.the-cma.org/french.html, et le document *Jouer sans se faire jouer* du Réseau Éducation-Médias, à l'adresse http://www.media-awareness.ca.

Mise à jour sur la protection de la vie privée

La vie privée dans les provinces et les territoires

Alberta
En 1999, on a étendu la *Freedom of Information and Protection of Privacy Act* provinciale aux municipalités et aux corps policiers. L'assemblée législative de la province a également adopté une nouvelle *Health Information Act* (abordée dans une autre section du présent rapport annuel), mais qui n'est pas encore entrée en vigueur.

Robert Clark, Commissaire provincial à l'information et à la vie privée, a statué en mai 1999 que l'Enquête sur la sécurité financière de Statistique Canada violait de façon déraisonnable la vie privée. En conséquence, Statistique Canada a changé de démarche et a conçu l'Enquête sur les dépenses des ménages. Avant de procéder, l'agence a demandé conseil au Commissariat et a informé clairement les personnes interrogées du fait que leur participation à l'Enquête était volontaire. De plus, le Commissaire mène activement un programme de sensibilisation dans les écoles et les collèges pour informer les jeunes Albertains au sujet de leurs droits à la protection des renseignements personnels.

Colombie-Britannique
David Loukidelis remplace David Flaherty au poste de Commissaire provincial à l'information et à la vie privée. M. Loukidelis, avocat de formation, est l'un des membres fondateurs de la British Columbia Freedom of Information and Privacy Association ; il est aussi le principal auteur du rapport sur la réforme législative qu'elle a publié, lequel a joué un rôle clé dans l'adoption de la *Freedom of Information and Protection of Privacy Act* provinciale.

Comme l'a recommandé le comité législatif spécial qui a passé cette dernière Loi en revue, l'assemblée législative provinciale a mandaté un comité spécial pour explorer les options de protection de la vie privée dans le secteur privé provincial. Le comité spécial mène actuellement des audiences publiques et accepte les mémoires afin de déterminer de quelle façon la province peut le mieux répondre aux besoins en matière de protection de la vie privée de ses citoyens.

Le problème du secteur public qui préoccupe le plus le Commissariat

provincial à l'information et à la vie privée est la prolifération de systèmes de surveillance vidéo, comme ceux que l'on se propose d'installer à Kelowna et à Vancouver afin de maintenir l'ordre public. Le Commissariat croit qu'on ne devrait installer de système de surveillance vidéo que si cette mesure est justifiée par des raisons probantes et extraordinaires dans chaque endroit proposé, et que ce genre de système constitue le seul moyen viable et efficace de décourager et de détecter les activités illégales. Le Commissariat prévoit surveiller l'usage des systèmes de Kelowna et de Vancouver tant pour s'assurer qu'ils sont conformes à la *Freedom of Information and Protection of Privacy Act* provinciale que pour prévenir la collecte non autorisée de renseignements personnels.

Manitoba

Le Bureau de l'ombudsman du Manitoba a reçu un nombre de plaintes de plus en plus important depuis l'adoption de la *Loi sur les renseignements médicaux personnels* (décembre 1997) et de la *Loi sur l'accès à l'information et à la protection de la vie privée* (mai 1998). Il a déposé son premier rapport spécial depuis l'entrée en vigueur des lois, lequel s'intitule A Privacy Snapshot... Taken September 1999. Ce rapport a nourri un débat public sur les enjeux relatifs à la vie privée auxquels font face quotidiennement les Manitobains. Le Bureau a également commencé à travailler sur deux outils analytiques fondés sur le rendement qui permettront de vérifier la conformité avec la Loi : un outil d'étude d'impact sur la vie privée et un outil d'évaluation des pratiques d'accès. Les essais pilotes de ces outils devraient être terminés en 2000. Pour remplir les obligations de sa charge, qui consistent à informer le public au sujet de la loi provinciale sur l'accès et la protection de la vie privée, le Bureau lancera son site Web au printemps 2000.

À compter d'avril 2000, les organismes publics locaux du Manitoba (organismes d'enseignement et de soins de santé et administrations municipales) relèveront de la *Loi sur l'accès à l'information et à la protection de la vie privée*, qui aura alors pleine force exécutoire.

Ontario

La loi sur la protection des renseignements médicaux personnels que propose et que retarde depuis longtemps le ministère de la Santé semble faire l'objet de révisions supplémentaires. Il se pourrait même que son adoption soit reportée davantage si le gouvernement envisage de l'intégrer dans une nouvelle loi provinciale sur le secteur privé, en réaction au projet de loi fédéral sur la protection des renseignements personnels dans le secteur privé.

Autre initiative dont les répercussions sur la vie privée sont importantes : la nouvelle carte à puce gouvernementale à usages multiples, qui a été annoncée

dans le Discours du Trône de l'automne 1999. La Commissaire ontarienne à l'information et à la vie privée a immédiatement communiqué avec le gouvernement provincial, lequel s'est engagé à mener des consultations exhaustives et ouvertes avec la Commissaire tout au long du projet.

Par ailleurs, la Commissaire a participé à des groupes de travail dirigés par le ministère ontarien des Transports pour intégrer des dispositifs de protection de la vie privée aux projets d'installation de caméras de surveillance du respect des feux rouges. Dans la même foulée, la Commissaire a commencé à travailler avec le ministère du Procureur général sur les impacts du projet provincial de justice intégrée sur les droits d'accès et à la vie privée. La Commissaire a également commencé à collaborer avec le ministère américain de la Justice à l'élaboration de principes de respect de la vie privée dans la conception de systèmes de justice intégrée.

Enfin, la Commissaire a été consultée et a formulé des commentaires au sujet des nouvelles lignes directrices sur les études d'impact sur la vie privée proposées par le Secrétariat du Conseil de gestion de la province.

Québec

La Commission d'accès à l'information du Québec a publié un outil pédagogique intitulé *Inforoute, attention : zone scolaire*. Ce guide a été conçu à l'intention des élèves des écoles primaires et secondaires du Québec qui utilisent l'Internet afin de leur apprendre à naviguer sur le Web en toute sécurité. Le guide propose également des paramètres de navigation sécuritaire aux enseignants et aux directeurs, que l'on exhorte à concevoir des procédures et des sites qui protégeront les enfants. Enfin, le guide aide les parents à mieux comprendre les répercussions qu'ont les nouvelles technologies sur leur vie privée.

La Commission a analysé une entente d'échange d'information conclue par le ministère provincial du Revenu et une maison de sondages privée à qui l'on a confié la tâche d'évaluer l'efficacité de son programme d'exécution des ordonnances alimentaires. La Commission a statué que le Ministère avait violé tant sa loi habilitante que la loi provinciale sur la protection de la vie privée dans le secteur public. Le Ministère s'est alors vu ordonné de récupérer et de détruire tous les renseignements qu'il avait obtenus de la maison de sondages ainsi que les données recueillies par cette dernière au cours de l'évaluation. Après cette intervention, la Commission a publié à l'intention de tous les organismes provinciaux des exigences minimales relatives aux sondages effectués directement par ceux-ci ou avec l'aide d'entreprises privées.

Enfin, la Commission a terminé l'implantation de son nouveau processus d'audience des plaintes ne pouvant pas être soumises à un arbitrage. Au 31 janvier 2000, la Commission avait entendu plus de 25 plaintes de ce genre.

Saskatchewan
Gerry Gerrand remplace Derrill McLeod au poste de Commissaire provincial à l'information et à la vie privée. M. Gerrand travaille pour le cabinet juridique Gerrand, Roth et Johnson et remplit également les fonctions de Commissaire provincial aux conflits d'intérêts.

La vie privée de par le monde

Un projet australien qui renaît de ses cendres
Au milieu des années 1990, l'Australie semblait prête à adopter une loi fédérale sur la protection des renseignements personnels dans le secteur privé. Mais le projet est mort en 1997 lorsque le premier ministre au pouvoir a manqué à sa promesse électorale en rejetant la recommandation de son procureur général en faveur de l'adoption d'une telle loi. Le gouvernement a ensuite encouragé les entreprises à s'auto-réglementer, une décision qu'ont dénoncé les défenseurs du consommateur et de la vie privée, qui ont réussi à raviver le débat

Pour aider les entreprises à s'auto-réglementer, la Commissaire australienne fédérale à la vie privée de l'époque a élaboré huit principes de protection de la vie privée inspirés des Lignes directrices de 1980 de l'Organisation de Coopération et de Développement Économiques. Certains états australiens ont tout de même poursuivi leur propre campagne de protection des renseignements personnels par le secteur privé. Les entreprises australiennes ont alors commencé à craindre qu'un ensemble de normes disparates ne surgisse si le gouvernement fédéral refusait d'intervenir. Elles craignaient aussi que la mise en œuvre de la Directive relative à la protection des données de l'Union européenne ne nuise à l'Australie si une loi n'était pas adoptée.

Le gouvernement de l'Australie a donc une nouvelle fois promis d'édicter une loi sur la protection des renseignements personnels dans le secteur privé. Cependant, cette loi se fonderait sur les huit principes de l'ex-Commissaire australienne fédérale à la vie privée lesquels, de l'avis du comité sénatorial australien des références juridiques et constitutionnelles, sont « faibles et fragmentaires » et comportent de « sérieuses lacunes ». La loi australienne reconnaîtrait les codes d'auto-réglementation en matière de protection de la vie privée, lesquels s'appuieraient sur les principes ci-dessus et seraient

approuvés et surveillés par le Commissaire à la protection de la vie privée. Si une entreprise ou une industrie ne rédigeait pas son propre code, le régime de traitement des plaintes prévu par la Loi, et géré par le Commissaire, s'appliquerait.

Le 30 novembre 1999, le procureur général de l'Australie a annoncé son intention de consulter à nouveau le public au cours des mois suivants et de déposer un projet de loi en l'an 2000.

Directive européenne : une épine sortie du pied américain

L'entrée en vigueur en octobre 1998 de la Directive relative à la protection des données de l'Union européenne signifie que les pays membres de l'UE ne peuvent plus communiquer de renseignements personnels sur leurs citoyens aux pays non membres qui ne protègent pas adéquatement ces renseignements. Le Canada et les États-Unis d'Amérique sont de ces derniers, mais notre Loi C-6 répondra probablement aux exigences de l'UE. La *Privacy Act* américaine est en vigueur depuis 1974, mais ne s'applique qu'aux organismes du gouvernement fédéral (à l'instar de l'actuelle *Loi sur la protection des renseignements personnels* canadienne). Le secteur privé américain n'est pas réglementé à l'heure actuelle et tient à ce que les choses demeurent ainsi ; les entreprises craignent l'immixtion de l'état et croient que la réglementation de la protection des renseignements personnels constituerait un fardeau inutile qui étoufferait la libre entreprise. En vue d'éviter une guerre commerciale transatlantique avec l'un des principaux partenaires commerciaux de l'Europe, les responsables de l'UE ont accepté de négocier avec leurs homologues américains pour parvenir à une solution mutuellement acceptable.

Le rapport annuel de l'an dernier décrivait la proposition américaine d'établir certains « refuges ». Sur acceptation, l'UE considéreraient que certaines entreprises américaines (et non l'ensemble du pays) offrent une protection « adéquate » si elles respectent un ensemble de principes volontaires de protection des données. Ces principes exigeraient que l'entreprise décrive à ses clients comment elle traite et échange les renseignements à leur sujet. Les responsables de l'UE n'ont pas rejeté la proposition américaine, mais ont demandé deux garanties supplémentaires : leurs citoyens devraient pouvoir accéder à tous les renseignements qu'une entreprise américaine détient à leur sujet et il devrait y avoir des mécanismes adéquats et accessibles permettant aux citoyens de l'UE de faire observer les règles américaines. Bien entendu, le mécanisme américain d'exécution de la loi est le recours aux tribunaux (un processus long et coûteux). Les pays de l'UE font quant à eux observer les règles de protection des données en nommant des Commissaires indépendants qui ont l'autorité d'ordonner des mesures correctives sans qu'il

en coûte quoi que ce soit aux plaignants.

Les pourparlers entre les deux parties se sont détériorés en décembre 1998. Une première échéance, fixée au 30 avril 1999, est passée sans qu'un accord n'ait été conclu, peut-être partiellement à cause du manque d'appui de la part des entreprises américaines pour la proposition de « refuge » du ministère américain du Commerce. Ces entreprises craignent que cette proposition n'entraîne l'adoption par leur pays d'une loi nationale sur la protection des renseignements personnels, ce à quoi elles s'opposent. La deuxième échéance, fixée au 21 juin 1999, n'a rien apporté de mieux, les deux principaux points de désaccord étant l'accès des consommateurs de l'UE aux renseignements à leur sujet et les questions d'exécution. La nouvelle équipe de direction de l'UE a alors proposé un compromis selon lequel les tribunaux américains obligeraient le respect des principes de « refuges » pour les plaignants européens. La troisième échéance fixée en octobre 1999 (anniversaire de la Directive) a été reportée en décembre 1999 en raison du faible progrès des négociations. Aucun accord n'a été conclu, et les négociateurs ont misé sur une nouvelle échéance de mars 2000.

Alors que nous allons sous presse, nous apprenons que les deux parties ont conclu un accord préliminaire qui voit l'UE se rallier au concept de « refuges ». Ce dernier ne s'appliquera cependant pas au secteur financier, que couvrira bientôt une nouvelle loi américaine spécifique. Cet accord préliminaire doit encore recevoir l'aval des deux gouvernements et pourrait entrer en vigueur dès cet été. Les défenseurs du consommateur et de la vie privée continuent toutefois de s'opposer à la notion de « refuges ». Ils favorisent la Directive plus normative, restrictive et davantage au service du consommateur. Les responsables de l'UE ont promis qu'ils annuleraient l'accord conclu avec les Américains dans l'éventualité où ces derniers ne l'appliqueraient pas comme il se doit.

Autres nouveautés

En **Autriche**, une nouvelle loi sur la protection des données personnelles est entrée en vigueur en janvier 2000, remplaçant celle de 1980 et reflétant les dispositions plus strictes de la Directive de l'Union européenne. La **République tchèque** vient d'adopter un projet de loi sur la protection de la vie privée qui rend illégal la collecte de renseignements sur des personnes sans leur consentement. Le sénat devrait approuver le projet de loi, qui prévoit aussi la création d'un nouveau Commissariat aux renseignements personnels, qui s'apparente un peu à d'autres commissions nationales de protection de la vie privée ou des données. L'**Afrique du Sud** vient également d'adopter un projet de loi sur la promotion de l'accès à l'information qui donne aux individus l'accès aux renseignements du

gouvernement (y compris aux données à leur sujet). Cette mesure fait partie d'un ensemble de quatre lois visant la mise en œuvre de la Déclaration sud-africaine des droits et portant un dernier coup au régime d'apartheid. En **Corée du Sud**, la nouvelle loi sur la promotion et la protection de l'infrastructure de l'information, en vigueur depuis le 1er janvier 2000, régit la collecte, l'usage et la divulgation de renseignements personnels dans les télécommunications et le commerce électronique.

Vue d'ensemble

Avec l'adoption de la Loi C-6, le Canada rejoint les rangs des pays de plus en plus nombreux à protéger les renseignements personnels de leurs citoyens dans le secteur public et, dans la plupart des cas, dans le secteur privé aussi. Les pays s'y prennent de l'une des deux façons indiquées ci-dessous.

Il y a d'abord les pays qui reconnaissent la protection de la vie privée — sous une forme ou une autre — comme un droit fondamental inscrit dans leur constitution ou d'une autre loi générale. Dans ce groupe figurent l'Argentine, la Belgique, le Brésil, la Bulgarie, le Chili, la République tchèque, le Danemark, l'Estonie, la Finlande, la Grèce, la Hongrie, l'Islande, Israël, l'Italie, le Japon, la Corée du Sud, la Lettonie, la Lituanie, le Luxembourg, le Mexique, les Pays-Bas, la Nouvelle-Zélande, le Pérou, les Philippines, la Pologne, le Portugal, la Russie, la République slovaque, la Slovénie, l'Afrique du Sud, l'Espagne, la Suède, la Thaïlande, la Turquie et certains états américains comme la Californie. Au Canada, le Québec est la seule province à reconnaître la protection des renseignements personnels de ses citoyens comme un droit fondamental inscrit dans son *Code civil*.

Il y a ensuite les pays qui ont adopté des lois spécifiques sur la protection des renseignements personnels ou de la vie privée (certains de ces pays peuvent figurer dans la liste susmentionnée). Ce deuxième groupe comprend l'Australie (dont certains de ses États comme la Nouvelle-Galles du Sud), l'Autriche, la Belgique, le Brésil, la zone administrative spéciale de Hong Kong qui appartient à la Chine, la République tchèque, le Danemark (y compris le Kalaallit Nunaat, anciennement le Groenland), l'Estonie, la Finlande, l'Allemagne (et tous ses *Länder*), la Grèce, la Hongrie, l'Islande, l'Irlande, Israël, l'Italie, le Japon (y compris certaines des ses préfectures comme celle de Tokyo), la Corée du Sud, la Lituanie, le Luxembourg, Monaco, les Pays-Bas, la Nouvelle-Zélande, la Norvège, la Pologne, le Portugal, la Russie, Saint-Marin, la République slovaque, la Slovénie, l'Espagne, la Suède, la Suisse (et tous ses cantons), Taïwan, la Thaïlande, le Royaume-Uni (y compris les îles autonomes de Guernesey, de Jersey et de Man) et les États-Unis d'Amérique (notamment certains États comme Hawaii ou New York). Au Canada, toutes les provinces (sauf

l'Île-du-Prince-Édouard) ainsi que les territoires ont une loi sur la protection des renseignements personnels.

Pour de plus amples renseignements sur les pays susmentionnés ou sur la Loi C-6, veuillez communiquer avec nous ou visiter notre site Web.

Ce que nous apprennent les journaux

GE Investments, division de l'assurance et des placements de la General Electric, a secrètement enregistré l'identité de milliers d'investisseurs qui ont répondu à une enquête postale sur leurs renseignements financiers personnels menée en 1998. Dans le cadre de l'enquête, on ne demandait pas aux répondants de fournir leur nom et leur adresse.

DoubleClick Inc., plus grande entreprise de publicité sur l'Internet en importance, a remis à plus tard son projet de relier des renseignements personnels aux données anonymes qu'elle recueille sur les internautes.

Un vaste groupe d'entreprises allant de Compaq à Oracle, en passant par Net Perceptions et Andromedia, travaillent à l'élaboration d'une nouvelle norme appelée « Customer Profile Exchange » (système d'échange d'informations personnelles sur les clients). Cette norme est conçue pour intégrer les données en ligne et hors ligne sur la clientèle que pourront utiliser les entreprises qui veulent recueillir des renseignements sur les consommateurs. Les registres de cadeaux en ligne permettent à une entreprise de recueillir de l'information sur l'acheteur et le destinataire.

Un programmeur parisien est accusé de contrefaçon et de fraude. En effet, il semble qu'il ait mis au point une « carte à puce » maison qui, selon lui, lui a permis d'acheter frauduleusement des produits et services dans toute la France.

Le service américain des douanes utilise le dispositif BodySearch dans plusieurs grands aéroports pour détecter la contrebande. Le mécanisme émet des rayons X à faible dose pour scruter un voyageur et affiche la silhouette nue de la personne.

Chaque fois qu'un étudiant déjeune ou franchit la porte d'entrée des résidences de l'Université de l'État de l'Ohio, un nouveau système d'accès par carte d'identité enregistre son nom dans une base de données ainsi que la date et l'heure du geste qu'il a posé.

Suite à des reportages dans les médias et à un recours collectif en justice, RealNetworks a cessé de saisir et de surveiller les données de ses clients — à leur insu — révélant les fichiers musicaux que ces derniers ont téléchargés du Web. TRUSTe, qui sanctionne officiellement les pratiques de sites Web en matière de vie privée, avait certifié les énoncés de confidentialité publiés par RealNetworks sur son site comme étant acceptables. TRUSTe a cependant refusé de se pencher sur le dossier, le geste contesté de RealNetworks reposant sur un logiciel, élément non couvert par la certification.

Une entreprise new-yorkaise du nom de American Student Lists obtient des données sur les étudiants provenant de permis de conduire, d'annuaires étudiants, d'abonnements à des revues, des éditeurs de livres de l'année, de fournisseurs de bagues de finissants, de fabricants de tenues de soirée, de restaurants à service rapide et de clubs de livres. Le commerce de données sur les étudiants qui en découle a donné lieu à un certain nombre de programmes de bourses fictifs visant les étudiants immigrants, qui font partie de groupes minoritaires et qui habitent en région rurale.

En août, la sécurité du service gratuit de courriel Hotmail de Microsoft — qui compte plus de 2,5 millions d'utilisateurs au Canada — a été compromise. À cause de cette lacune, un utilisateur non autorisé aurait pu lire, supprimer et faire suivre les messages d'un autre utilisateur, simplement en devinant son nom d'accès.

À l'occasion d'une récente foire commerciale, la General Electric a présenté le concept du « réfrigérateur Internet », capable de lire les codes barre des produits que l'on y entrepose et de les recommander au besoin. À la même

occasion, la société Whirlpool a présenté un réfrigérateur qui dresse instantanément une liste d'épicerie. Ce réfrigérateur peut repérer les aliments et offre une tablette sans fil qui permet aux consommateurs de télécharger des recettes de l'Internet.

Depuis quatre ans, Mobiltrak, entreprise de Birmingham (Alabama), vend un dispositif qui détecte quelles stations de radio les gens écoutent dans leur auto. Les clients de la compagnie payent l'installation du dispositif dans l'entrée de leur entreprise. Ce dernier, de la taille d'une boîte à chaussures, détecte les signaux en provenance de l'oscillateur d'une voiture, lequel syntonise la fréquence radio désirée. Les données recueillies sont acheminées à Mobiltrak, laquelle envoie alors un rapport à ses clients dans lequel ces derniers peuvent vérifier s'ils font diffuser leurs publicités sur les bonnes stations de radio.

Au début de l'an prochain, le Maryland et la Virginie commenceront à mesurer la congestion routière en suivant les automobilistes qui parlent sur leur téléphone cellulaire pendant qu'ils sont sur la Capital Beltway. La compagnie U.S. Wireless rajoutera de son équipement aux relais cellulaires actuels pour suivre les signaux des automobilistes et en faire un relevé cartographique.

Acxiom Corp., entreprise de l'Arkansas qui fournit des renseignements aux spécialistes en marketing, a accumulé 135 millions de numéros de téléphone de consommateurs — y compris près de 20 millions qui ne figurent pas dans les annuaires — pour contribuer à identifier les gens qui achètent ou se renseignent par le biais de numéros sans frais, et à dresser leur profil.

La police écossaise prélève un échantillon d'ADN de toute personne arrêtée, même pour une simple infraction au code de la route. De plus, l'Association internationale des chefs de police a demandé au Congrès américain d'exiger

que l'on prélève un échantillon d'ADN de toute personne arrêtée, et Rudolph Giuliani, maire de la Ville de New York, a demandé que la législature de l'état du même nom exige le prélèvement d'échantillons d'ADN de tous les nouveau-nés. Une loi de la Louisiane qui est entrée en vigueur le 1er septembre 1999 exige que l'on prélève un échantillon d'ADN des personnes accusées — mais pas nécessairement reconnues coupables — d'un crime violent.

En décembre, la U.S. Food and Drug Administration a ordonné à l'Université Commonwealth de Virginie de suspendre la plupart de ses projets de recherche médicale jusqu'à ce qu'elle prouve qu'elle a amélioré ses mesures de protection de la vie privée et de la sécurité des sujets de ses recherches.

Un recours collectif sans précédent contre CVS Pharmacy Inc. et de grands fabricants de produits pharmaceutiques a été annoncé en novembre. On y allègue que CVS a utilisé certains renseignements personnels sur ses consommateurs contenus dans sa base de données centrale pour cibler un programme de marketing postal direct financé et dirigé par les autres compagnies pharmaceutiques accusées.

À l'hôpital St. Joseph's Mercy à Pontiac, au Michigan, le public pouvait accéder à certains dossiers médicaux confidentiels parce que le système n'exigeait pas des utilisateurs qu'ils entrent un mot de passe ou un autre code de sécurité… Le système de l'hôpital utilise un service interne de dictée numérique qui permet aux médecins d'enregistrer des notes concernant les consultations et les examens récents des patients et d'y accéder. Les notes comprennent l'information sur les patients, allant des données sur l'admission et le congé jusqu'au dossier sur la santé cardiaque et mentale.

Des chercheurs de l'Université de la Californie à Berkeley construisent un minuscule robot de la taille et de la forme d'une mouche qui sera utilisé pour la surveillance.

Dans le cadre d'un programme de dépistage des drogues mené en août dernier auprès des automobilistes, les policiers du Québec ont demandé à des automobilistes choisis au hasard à divers points de vérification de la province de se ranger au bord de la route. Ensuite, des étudiants en sciences infirmières demandaient aux conducteurs s'ils voulaient donner volontairement un échantillon de salive ou d'urine pour le dépistage de drogues ou — même si ce n'était pas l'objectif premier de l'étude — d'alcool. Si les automobilistes refusaient, ils pouvaient reprendre la route, et s'ils acceptaient et que les résultats des tests révélaient qu'ils étaient sous l'influence de drogues ou de l'alcool, aucune pénalité ne leur était imposée.

Be Free, entreprise de marketing en ligne, a reçu un deuxième brevet pour certaines méthodes qui permettent de dresser le profil des consommateurs selon leurs préférences. Ce brevet est différent du premier en ce sens qu'il inclut des techniques de profil anonyme.

Le 10 décembre 1999, Applied Digital Solutions Inc. a acquis les droits de brevet pour une technologie qu'elle appelle « Digital Angel ». Digital Angel est un émetteur-récepteur que l'on peut implanter dans le corps humain. Il est activé par l'énergie électromécanique, c'est-à-dire le mouvement des muscles, et peut demeurer implanté et fonctionnel pendant des années. Il peut être activé soit par celui qui le porte, soit par un système de surveillance à distance. L'appareil peut également surveiller certaines fonctions biologiques du corps humain — comme la fréquence cardiaque — et envoyer un signal de détresse à un système de surveillance lorsqu'il détecte une urgence médicale. Des satellites peuvent suivre à tout instant l'emplacement exact de l'appareil.

Un nouveau système de sécurité mis au point en Grande-Bretagne permet d'identifier les gens par leur seule démarche.

À San Francisco, une nouvelle boutique Levi's vient d'entreprendre une vaste collecte volontaire de données biométriques à des fins de mise en marché. La boutique encourage ses clients à faire enregistrer leurs empreintes digitales et leurs renseignements personnels dans une base de données. La boutique rajoute ensuite les goûts musicaux des clients en fonction de la durée d'écoute de certaines chansons aux bornes musicales de la boutique. Les clients peuvent également entrer dans une cabine privée munie d'un dispositif qui crée une image tridimensionnelle de leur corps afin de suggérer une taille appropriée de jeans : c'est la « Levi's Original Spin ». Les dimensions sont rajoutées aux données des clients.

Gestion intégrée

Même s'ils partagent locaux et services administratifs, le Commissariat à la protection de la vie privée et le Commissariat à l'information fonctionnent de façon indépendante en vertu des lois habilitant leurs opérations. Par souci d'économie et d'efficacité pour le gouvernement et les programmes, ces services (finances, personnel, informatique et administration générale) sont centralisés au sein de la direction de la Gestion intégrée. La direction compte un personnel de 15 employés seulement (qui exercent diverses tâches) et un budget représentant environ 14 p. 100 du budget total des dépenses de programme.

Description des ressources

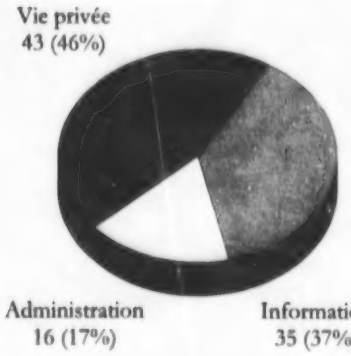
La gestion innove constamment dans la prestation des services sans pour autant diminuer la qualité des services offerts au public. À leur réunion d'avril 1998, les Ministres du Conseil du Trésor ont approuvé un examen des services votés afin d'examiner les niveaux de ressources des Commissariats ainsi que leurs besoins en technologie de l'information et de locaux. Les Commissariats ont utilisé ces ressources pour faire face aux augmentations de la charge de travail et s'acquitter de leurs mandats tout en maintenant les services essentiels.

Le budget combiné que les deux Commissariats avaient projeté pour l'exercice 1999-2000 s'élevait à 9 869 000 $. Les dépenses réelles pour le même exercice étaient de 9 760 574 $. De cette somme, 6 675 947 $ ont été affectés au personnel et 1 136 597 $ ont été versés en services professionnels spéciaux, soit plus de 80 p. 100 de toutes les dépenses. Le solde de 1 948 030 $ a été affecté à tous les autres coûts, y compris la poste, les télécommunications, les fournitures, l'équipement relié aux technologies de l'information ainsi que l'équipement de bureau.

Les dépenses sont ventilées au tableau 1 (par organisme / activité) et au tableau 2 (par type de dépense).

Tableau 1: 1999-2000 Ventilation par organisme / activité

Ressources humaines
(Équivalents temps plein)



Ressources financières
($000)

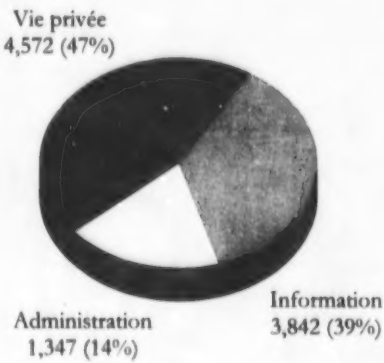


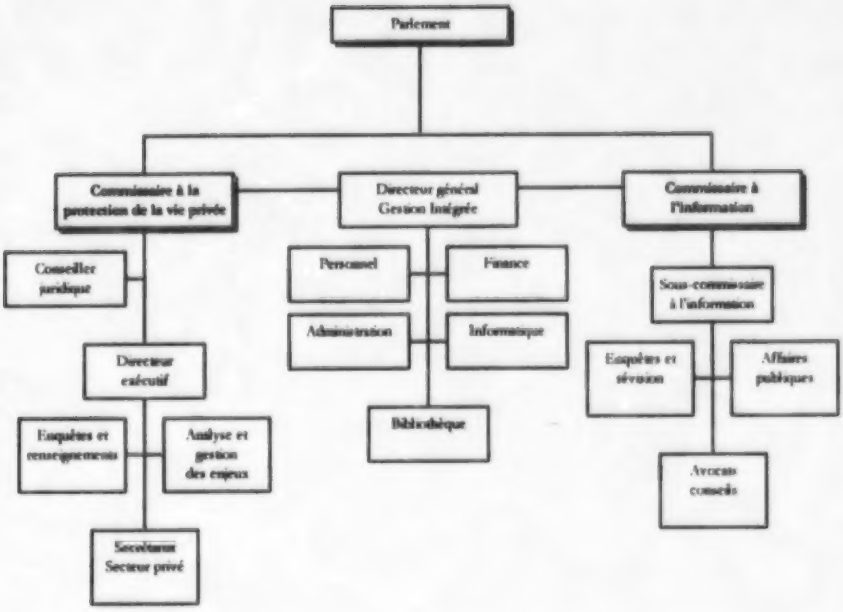
Tableau 2: Ventilation par type de dépense

pour l'exercice financier prenant fin le 31 mars 2000

	Information	Vie privée	Gestion intégrée	Total
Salaires	2 200 135	2 750 322	751 490	5 701 947
Contributions aux régimes d'avantages sociaux	388 000	453 000	133 000	974 000
Transports et communications	84 030	106 430	105 952	296 412
Information	66 329	27 999	1 735	96 063
Services professionnels et spéciaux	383 442	574 001	179 154	1 136 597
Locations	4 210	28 634	19 778	52 622
Achat de services et réparations	8 460	72 204	8 883	89 547
Services publics, approvisionnements, fournitures	29 883	32 729	45 692	108 304
Achat de machines et d'équipements	676 808	526 512	100 746	1 304 066
Autres paiements	900	116	0	1 016
Total	**3 842 197**	**4 571 947**	**1 346 430**	**9 760 574**

* Ces dépenses ne reflètent pas les rajustements de fin d'exercice indiqués aux Comptes publics des Commissariats pour 1999-2000.

Organigramme



Personnel du Commissariat

Mes années à la tête du Commissariat fédéral à la protection de la vie privée représentent à mes yeux un honneur et un privilège. Elles m'ont aussi apporté de nombreuses satisfactions, dont la plus importante reste celle d'avoir côtoyé un personnel hors pair et des plus professionnels. Je tiens ici à remercier tous ceux et celles qui m'ont apporté leur appui avec enthousiasme au cours des dix dernières années. Les voici donc, et que les personnes que j'aurais malencontreusement oubliées me le pardonnent :

* à l'emploi du Commissariat le 31 mars 2000
** en détachement à l'extérieur du commissariat le 31 mars 2000

Ackroyd, Jeanette
Anderson, Colleen
Aubry, Benoit
Baggaley, Carman *
Baker, Barry
Barbaro, Tony *
Bastedo-Boileau, Catherine
Beaulé, Claude *
Bedley, Robert *
Bell, John
Bergeron, Michelle *
Blais, Anne *
Bloomfield, Stuart *
Boileau, Louise
Brault, Anne-Marie
Brault, Raymond
Brown, Grace *
Brunet, Josée
Carnegie, Doug **
Cliche, Nicole
Coolen, Gary *
Delisle, Julien *
Doré, Richard **
Doyle, Kathryn *
Dubuc, Philip
Dubuc, Thérèse *
Eadie, Kim
Evans, Jocelyne *
Fagan, Mike *
Fanjoy, Monique *
Farley, Francine
Fitzpatrick, Tom *
Fong, Marcus
Foran, Brian *
Gauthier, Yvon
Goldsmith, Ann *
Gow, Glenn
Gravelle, Robert

Hamilton, Joanne *
Harris, Holly *
Hébert, Raymond *
Henry, Gary
Imbeault, Marie-Andrée *
Jackson, Sally
Khosla, Jay *
Kirkby, Hedy
Labelle, Louise *
Lacroix, Ginette
Lafleur, Ann Marie *
Lapierre, Don
Lavoie, Chantal *
Lavoie, Roxanne
Leblanc-McCulloch, Monique *
Lévis, Jacques *
Lystiuk, Fred *
Mann, Don
Martelock, Cathy *
Maurel, Richard-Philippe *
Maynard, Peter
McAuliffe, Ann
McLean, Joyce *
Ménard, Nicole *
Millar, Melanie *
Montigny, Gerry
Mullen, Dennis
Nantel, Martine *
Neary, Gerald *
Netterfield, Carolyn
Oscapella, Eugene
Pavlis-Gougeon, Virginia *
Perreault, Renée
Peszat, Jan *
Richard, Paul *
Richer, Michel
Rodrigue, Jocelyne *
Rooke, Anne *
Roy, Rachelle
Roy, Jocelyn
Savas, Eric
Schwartz, Virginia *
Scott, Pat
Sérafin, Nicole *
Sicotte, Nicole *
St-Pierre, Chantal *
Stewart, Brian *
Tessier, Isabelle
Thériault, Natalie *
Thibaudeau, Monique *
Trottier, Ghislaine
Van Berkel, Gerry
Welke, Ron
Wheeler, Susan *
Wolchuk, Ron